COMBINED SAFETY AND SECURITY RISK EVALUATION CONSIDERING SAFETY AND SECURITY-TYPE INITIATING EVENTS

A Thesis

by

MOHAMMAD ABDEL-MAJID MUSTAFA HAWILA

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	Sunil Chirayath
Committee Members,	Pavel Tsvetkov
	Laszlo B. Kish
Head of Department,	Yassin Hassan

December 2016

Major Subject: Nuclear Engineering

ABSTRACT

Destruction to critical nuclear infrastructures would have a debilitating effect on national public health safety, national economy, security, etc. For this reason, analysts perform safety risk analyses to quantify and understand the nature of unwanted events. Since the world has gone through many changes after the terrorist attacks of 9/11, nuclear security risk analysis became a necessity. So far, the safety and security risk analyses were done separately without a combined analyses and evaluation. This research thesis contains three major analysis sections that provides security, safety, and combined safety-security risk analysis that studied and analyzed possible accident scenarios.

This research starts with the security pathway analysis, which eventually calculated the initiating event frequency of a successful adversary attack and estimated the security risk value. The safety analysis represented a series of natural (random) safety systems failure events. On the other hand, the safety-security analysis considered a security initiating event followed by safety systems failure. Fault and event trees were formed using the SAPHIRE software and used for the description of failure scenarios.

The main outcome of this research is a methodology development to perform combined safety-security initiating event analysis to compute the joint top event system failure frequency. Along with the calculation of the systems' failure frequency, estimation of the public risk associated for sample failure scenarios, and the determination of how security initiating events in a series of safety events failure affect the total risk value was also carried out. Considering a security attack as an initiating event that triggers safety

system failure was analyzed for developing the methodology to perform a combined safety-security risk analysis estimation.

The analysis showed that the security attack substantially changed the risk value when it was considered in the failure process. This created a major need to consider both the security and safety failures together in the future systems for failure scenarios. More evaluations should be done to the security system measures to reduce the total associated risk value. Future efforts should look for further enhancements and development in the analysis of the deployed safety and security systems.

ACKNOWLEDGEMENTS

NOMENCLATURE

ASD   Adversary Sequence Diagram

DBT   Design Basis Threat

EASI   Estimate of Adversary Sequence Interruption

EDG   Emergency Diesel Generator

EPS   Emergency Power System

IE   Initiating Event

LOOP   Loss Of Offsite Power

NRC   Nuclear Regulatory Commission

PRA   Probabilistic Risk Assessment

PPS   Physical Protection Systems

PSA   Probabilistic Safety Analysis

SAPHIRE   System Analysis Programs for Hand-On Integrated Reliability

      Evaluations

SFP   Spent Fuel Pool

VESPA   Vulnerability Evaluation Simulating Plausible Attacks

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

1. INTRODUCTION

Safety and security design inclusion in nuclear fuel cycle facilities are mandatory by the operating country's regulatory agency. This is to minimize the probability of nuclear or radiological incidents or accidents, and hence, to keep the risk to the public and the environment below the acceptable limit. Design analyses performed for risk quantification ensure the adequacy of the safety and security measures at the nuclear fuel cycle facility. In this research, risk evaluation of an operating nuclear spent fuel pool (SFP) facility was performed considering both safety-type and security-type Initiating Events (IEs) to demonstrate the differences in performing a joint safety-security risk evaluation. The objective is to understand the benefits of employing a combined safety-security risk evaluation methodology.

Nuclear safety risk analysis is generally performed in three steps. The first step is to calculate the damage frequency of a critical system, for example the core damage frequency of a nuclear reactor using the event tree and fault tree techniques [1]. In this step, analysis on the progression of an IE, for example a valve failure leading to a top event such as reactor core damage, is carried out considering the failure frequency data of intermediate system elements. This step is followed by the radioactive source term estimation due to the potential system damage. The final step is the estimation of consequence in the public domain from the partial or total release of the radioactive source term to the environment. A system-of-systems analysis is then carried out to quantify system vulnerabilities, which if not addressed, could lead to undesirable events.

1

Deterministic and probabilistic approaches are commonly used in nuclear safety analysis for estimating the accident frequency using event and fault trees methods [2]. A probabilistic approach is used in this thesis research for the safety analysis and for the combined safety-security analysis to determine the failure frequency of the SFP. A different approach, namely, adversary sequence diagram (ASD) approach is used for the failure frequency from a security IE. Safety-type, security-type and a combination safety-security-type IEs are considered.

A security threat and the related IEs are not considered in the safety risk analysis approach currently used in the industry. Instead, the vulnerability of the physical protection system (PPS) is performed independently, even though the consequence resulting from a security or safety IE is in the same public domain. An attempt is made here to study the effect on the overall risk by considering security IE along with the subsequent random failure of the intermediate safety system elements that may lead to the top event.

Estimation of the security risk is made by utilizing the equation

$$R = P_A*(1- P_I *P_N)*C \qquad (1)$$

Where P_A: is the frequency of adversary attack, P_I: is the probability of interruption of the adversary by the PPS, P_N: is the probability of neutralizing the adversary by the response force, and C: is the consequence of the attack [3]. While the safety risk is determined (in its simple form) using the equation

$$R= F * C \qquad (2)$$

2

Where F: is the safety system failure frequency per year and C represents the undesired consequences similar to that of equation (1) [4]. Contrary to the security risk equation, F *does* describe the probability (a numerical measure of the likelihood that an event will occur) of a random, independent event. On the other hand, the security event represents a non-random IE. The consequence value C in both equations (1) and (2) is the same no matter what triggered a system failure (safety or a security IE), since it similarly affects the public domain. The proposition and development of a combined safety-security risk analysis methodology in this research was largely inspired by the shared consequence value.

In this research, a new methodology is presented to determine a combined safety-security frequency of an undesired event at a hypothetical SFP facility. The analysis includes the security attack at a SFP facility or its components as an initiating postulated event in addition to the random failure of the safety components.

1.1 Objectives

The main scope of the study is to analyze the differences in risk calculations due to the possible accident scenarios at a SFP by determining the failure frequencies from security-type, safety-type and combined security-safety-type IEs. The methodology under development is not specific to SFP but should be generally applicable to other nuclear fuel cycle facilities as well. The objective of the study is to understand the interplay between nuclear safety and security IEs in a nuclear fuel cycle facility so as to: (1) determine their

3

independent contributions to the public risk, and (2) determine whether there is value in performing a combined security-safety risk quantification arising from a security-type and safety-type IEs so that prudent resource allocations can be made.

1.2 Previous Work

A literature review shows diverse definitions of the terms security and safety [5, 6]. Many of the definitions present the distinctions between the two terms as: System vs. Environment and Malicious vs. Accidental. In the first distinction, security deals with risks from the environment over the system, while safety deals with risks from the system over the environment. Whereas per the second distinction, security attempts to mitigate the risk from malicious acts while safety addresses risk from accidents [7].

In another study, a methodology was addressed to enhance the synergies between safety and security [8]. Since the early time of nuclear industry, growing safety concerns became visible to the analyst; however, security was not a major concern. 9/11 and the growth of terrorism more recently brought security concerns onto the public agenda. In order to protect and prevent the loss of valuable assets, a PPS is deployed along with the existing safety systems. In the current analyses, safety and security systems are independently evaluated to determine the failure frequency of their related elements and the associated risk.

Various risk assessments have been done on safety and security IEs individually, but have never considered both as interconnected concepts. There are many approaches

for evaluating the effectiveness of a security system from a strictly security IE perspective. One is called the Vulnerability Evaluation Simulating Plausible Attacks (VESPA). VESPA provides a what-if scenarios-based comparative tool for the selection of plausible targets that, from the perspective of a terrorist, present a high potential of certain vulnerabilities to be exploited [9]. Another approach for studying security and safety that can be found in the literature is analyzing the system through the insider (the person who has access to sensitive locations in the nuclear facility), in which a person can bypass the security measures, or collude with outsiders to harm the safety systems [10, 11]. Game theory approach is another method which serves the risk analysis assessment process. The outcome from the game theory helps in examining how the PPS functions when attacked by a knowledgeable adversary with insider help at a hypothetical nuclear facility [12]. While these approaches are entirely focused on security, they neglect safety.

Safety is also given individual analysis. A technical study of SFP accident risk by the Nuclear Regulatory Commission (NRC) published in 2001 works as a basis for analyzing the failure process of SFP. The study provided risk assessment for severe accident scenarios and estimated their consequences. For a given set of fuel characteristics, the time required to boil off enough water that allows fuel rods to reach high temperature that initiate zirconium cladding fire was estimated by the study. The summary of the study was that the risk of a SFP accident that leads to a zirconium fire was low, despite the large consequences [13]. This study, however, gave no attention to security risk, and currently there is no consideration for a safety-security joint risk analysis and evaluation for a failure

5

event. In summary, previous and current safety and security risk analyses are done separately without considering the synergies in both risk analyses.

1.3 Methodology and Procedure

The nuclear fuel cycle facility selected for the current study is a SFP, which allows for the analysis of public risk arising from the interplay between nuclear security-type and safety-type IEs. The EASI (Estimate of Adversary Sequence Interruption) model is used to calculate the security IE frequency leading to the failure of a safety component [3]. Further progression of this security IE to a top event is analyzed using a probabilistic safety analysis (PSA) tool, called the System Analysis Programs for Hand-On Integrated reliability Evaluations (SAPHIRE, version 8), to obtain a combined pool damage frequency [14]. For the progression of events leading to a top event, the failure of the intermediate safety elements is assumed as natural random-type failures. The objective is to compare the pool damage frequency estimated from a security IE to that of a safety IE and vice versa.

Additionally, a security sabotage event and a safety-type only IE at the SFP is analyzed. At least one adversary path to the SFP is analyzed from the security side, addressing the detection and delay elements of the PPS with their respective values of probability of detection (P_D) and time delay (t_D). The response force time was estimated with the assumption that the response force will travel by foot. These elements and values lead to the calculation of the probability of interruption, P_I, one of the terms needed to

assess the security vulnerability (refer to equation (1)). The vulnerability of a security path is called the probability of adversary success (Ps), which is equal to (1- P_I*P_N). Adversary success probability times the frequency of attack per year gives the frequency of a successful security attack. This frequency is used in the combined safety-security analysis the security IE failure frequency.

Probabilistic Risk Assessment (PRA) Level-1 is used for the safety analysis and the combined safety-security analysis in this research to calculate the associated combined failure frequency of the system. The safety analysis represents a series of natural safety system failure events. On the other hand, the safety-security analysis considers a security IE followed by safety system failures. The PRA analysis includes fault and event trees formation, which is used for the description of failure scenarios from the basic event to the top event and calculation of the related frequency of failure of the analyzed system elements. The event and fault trees are created using the SAPHIRE software to assist the risk evaluation process of the chosen system failure scenarios from IEs of safety-type and security-type.

The tasks of the research are:

1. Develop a simple hypothetical SFP layout.

2. Conduct a security analysis to the SFP layout in order to calculate the security parameters such as the probability of interruption, probability of neutralization, frequency of attack, and the associated risk.

3. Identify the possible IEs including security attack as external event.

4. Perform safety risk analysis Level-1 PRA for the cooling system component of the SFP for natural random failure events.

5. Conduct combined safety-security analysis for the cooling system components of the SFP, considering the security attack as an IE.

6. Create event and fault trees using SAPHIRE 8 software included in safety analysis, and safety-security joint analysis.

7. Calculate safety system failure frequency and joint safety-security failure frequency.

8. Calculate the associated risk value for each case of safety-type, security-type and joint security-safety-type IEs.

1.4 Significance of Work

The significance of this research is that it identifies a methodology for calculating a combined safety-security failure frequency and combined risk value that could serve as the basis of efficient risk analysis process security-type and safety-type IEs. The combined analysis process will improve the evaluation of the deployed safety and security systems in any nuclear facility. As a result, it will provide a combined failure frequency which considers the safety and security interface, as well as a better estimation of the risk value. The new combined risk evaluations methodology will lead to a balanced risk evaluation so that resources can be better allocated at the safety and security system levels.

1.5 SFP (Target) Characteristics and Accidents Consequences

Each year, U.S. nuclear power plants generate about 2,000 metric tons of spent fuel with an accumulative amounts of 65,000 metric tons since the start of nuclear power generation [15]. Almost 75% of the spent fuel in the U.S is stored in SFPs to reduce its deadly effects. A SFP is used to store the spent fuel temporarily because the radioactive isotopes in the spent fuel produce heat continuously as a result of the decay process. Safe storage of the spent fuel in pools requires its continued cooling at least first 5 years. Failure of this cooling leads to water vaporization, un-shielding the fuel and the risk of environmental radioactive release. About 1000 Sv/hr are produced from each spent fuel rod radiation per hour at a 1-foot distance from the rod; this amount of radiation is enough to end life in seconds [16]. This radiation comes from a wide variety of isotopes with long half-lives generated in the reactors during their normal operations. Table 1 summarizes the activity level of the main radiation isotopes that can be found in repository such as a spent fuel pool after a cooling period at least 5 years

Table 1 Spent fuel main radiation isotopes and percent activity [16]

Isotope	Half-life (years)	Percent Activity (%)
Cesium-137	30	38%
Plutonium-241	14	26%
Strontium- 90	29	25%
Cobalt -60	5.3	0.22%
Samarium-151	90	0.20%
Nickel-63	100	0.18%

According to Table 1 about 40 percent of the radioactivity in the spent fuel comes from cesium-137. Usually, the inventory at the spent fuel pools is more than the inventory at the reactors because the pools are designed with a capacity to absorb 2-3 time's reactors' contents, which represents a massive amount of radiation. The pools typically are designed in a rectangular shape about 45 feet deep, and the walls are made of reinforced concrete with a thickness about 4-5 feet and a stainless steel liner to resist cracks, breaks, and corrosion [16]. Fig. 1 shows a simple example of what the SFP looks like [17].

1.5.1 Cooling system function and components

Water flows to the spent fuel through scuppers at the normal water level, extracting the heat from the spent fuel. The water in the pool is circulated through a cooling system to remove the continuously produced decay heat that is produced by the radioactive isotopes in the spent fuel. Finally, the pool cooling system cools the water before injecting

it back into the pool. The water must be maintained at a certain level in the entire pool to guarantee continues operation of the cooling system. If the water were to rapidly drain from the pool, this will cause the cooling system to stop working.
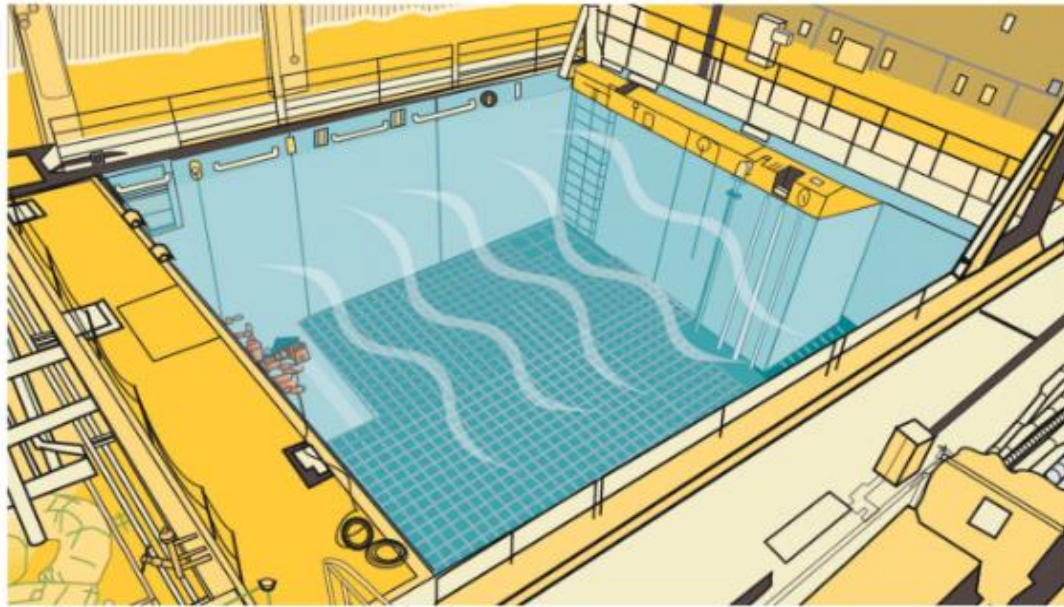
Fig. 1 Example of a commercial light water reactor SFP

Fig. 2 shows the hypothetical layout of the SFP and its components, which was prepared and used in this research for the safety risk analysis part that will be illustrated in one of the later sections. Based on Fig. 2, the SFP has a cooling system that is composed of a rectangular spent fuel pool, cooling pumps, valves, heat exchanger, makeup tank, reservoir, and filtration system.
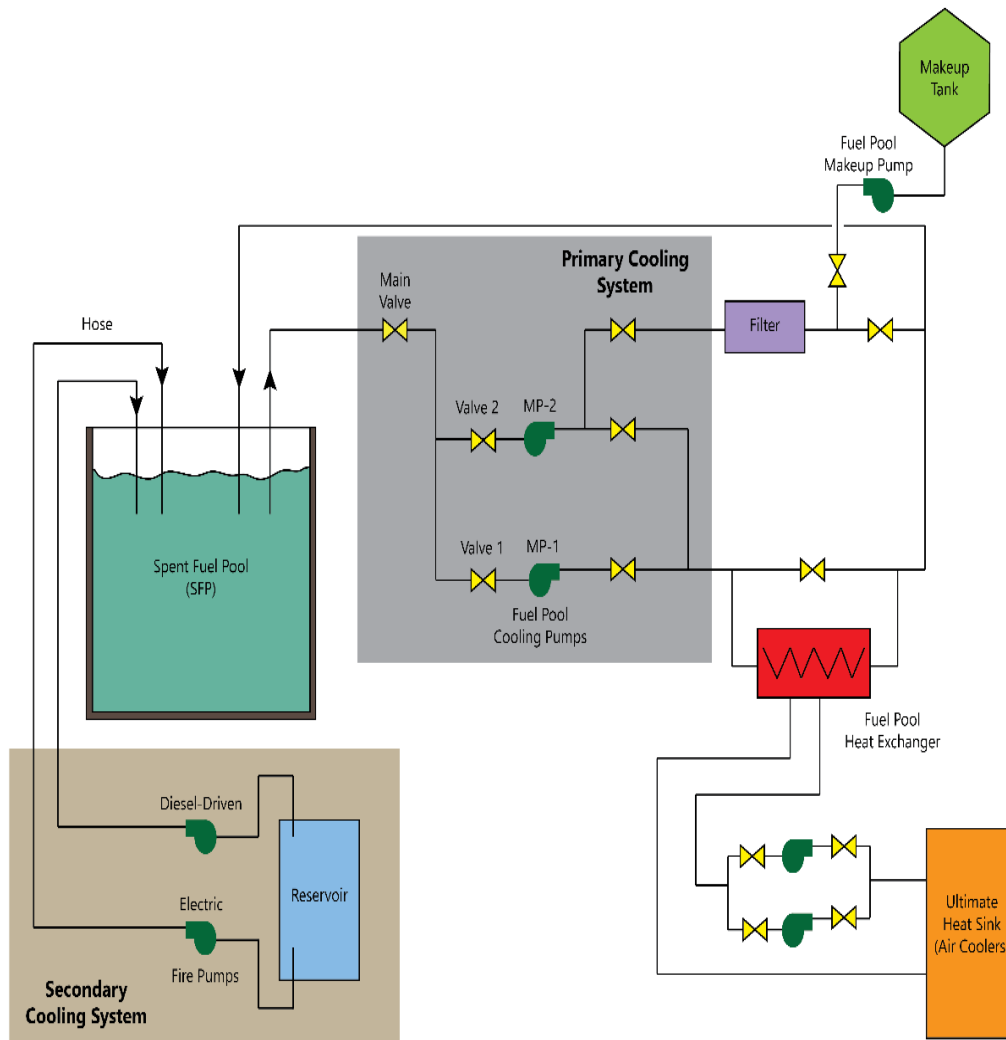
Fig. 2 SFP and cooling system component diagram

As is clear from the SFP layout, a cooling system is composed of two parts: the primary cooling system, and the secondary cooling system. The primary cooling system has two main pumps that reflect system redundancy in which one pump works at a time during normal operation and the other is reserved for an emergency situation. One of the pumps draws coolant from the SFP through a cooling pipe line, where two valves are

installed on each pipe line to control the process. The primary cooling system also has a valve installed on the main pipe line (main valve) that controls the water withdrawal from the pool. Then water is passed through a heat exchanger system to extract the heat, and cool it down to be returned to the pool. The heat exchanger system is composed of a heat exchanger, and two redundant pumps with their respective valves. One pump works at a time that extracts the heat from the heat exchanger to the ultimate heat sink, and the other pump is reserved for emergency situations. In contrast, the secondary cooling system is composed of two pumps: a diesel driven pump and an electrical driven pump, which are installed over two independent pipelines to maintain independency and redundancy in the system. These pumps withdraw water from the reservoir and inject it into the SFP during abnormal and accident conditions

A small amount of water that passes through a filtration process is returned back to the discharge line. Though not analyzed in this research, a makeup water tank with a limited flow rate supplements the small losses due to evaporation by injecting water to the main line of the primary system. For large loss-of-coolant-inventory accidents, water addition through the makeup pumps does not successfully mitigate the loss of the inventory event unless the location of inventory loss is isolated. For safety purposes plants do not have drain paths in their SFPs that could lower the pool level more than 15 feet below the normal pool operating level [16].

1.5.2 SFP accident consequences

Any possible accident at the SFP, such as fire, a pipe breaking, etc., while it's loaded with radioactive sources could result in catastrophic consequences. Of the possible accidents, fire would result in a severe damage. It would contaminate with radioactivity about 188 square miles around the nuclear reactor, with 28,000 possible cancer fatalities and almost 59 billion dollars as a cost of the damage for a typical reactor power facility [16]. Any accident that expose the fuel to air and steam would cause the zirconium cladding to react exothermically, catching fire at about 800 degrees Celsius. The amount of the cesium-137 in spent fuel pools represents about 20 to 50 million curies of high penetrating radiation with a long half-life that could be totally released into the environment in case of a severe accident [16]. Making any accident happen at the SFP that lead to severe damages and radiation release is considered the main threat from a sabotage attack. Thus, preventing this requires deploying safety and security systems to make sure no severe accident will take place. Although elimination of accident probability is impossible, reducing it is possible.

2. SECURITY ANALYSIS

This section represents the pathway security analysis, which includes the complete security path analysis from the offsite area to inside the reactor facility up to the spent fuel pool. The main two security concerns are theft (nuclear or radioactive materials) and sabotage (process or support equipment). For this study, the focus was on the sabotage case. Analysis was on many possible adversaries' paths to sabotage the SFP target. Since the focus in this research is on the methodology of analysis and connecting security with safety, the only path included in this research thesis is the most vulnerable path (the path with the highest risk value). The main outcomes of the pathway security analysis is found by calculating the security parameters such as: the probability of interruption, the probability of neutralization, the security attack frequency, the consequence value related to the accident level, and estimating the associated path risk value. In order to understand the analysis concept, key terms are defined:

Risk: The potential for loss or harm due to the likelihood of an unwanted event and its adverse consequences. In security, risk is based on the analysis and aggregation of three widely recognized factors: threat, vulnerability, and consequence.

Consequence: The results of an event, which includes immediate, short- and long-term, direct and indirect losses. Loss may include human, environment, and economy, political and other impacts. The value of C used in this study is scaled from 0 to 1 representing the severity of the event.

Threat: Any indication, circumstance, or event with the potential to cause the loss of, or damage to, an asset or population.

Vulnerability: Any weakness in an asset's or infrastructure's design, implementation, or operation that can be exploited by an adversary. The weaknesses can occur in building characteristics, equipment properties, personnel behavior, locations of people, or operational and personnel practices [18].

2.1 SFP Security Path Analysis

The analysis carried out is to calculate the vulnerability parameters of a security pathway, which is the probability of interruption and probability of neutralization (P_I, and P_N respectively). P_I calculation is through the EASI excel model [3] and the P_N calculation is by using excel sheet macro [19]. Fig. 3 and Fig. 4 show examples of what the EASI model and P_N excel sheet respectively look like.

Fig. 3 Example of the EASI model layout [3]

Fig. 4 Example of excels macro sheet layout, which is used for P_N calculation [19]

2.1.1 Physical protection measures

The SFP assumed to be in full capacity contains radioactive nuclear spent fuel assemblies, which are especially attractive sabotage target due to the severity of radiological consequence. For this reason, several protection layers exist between the valuable assets and the offsite area. The hypothetical facility site diagram and the layout

of the SFP location that is used in the pathway security analysis are shown in Figs. 5-6 (In

the figures below, each P# represents a door) [20].
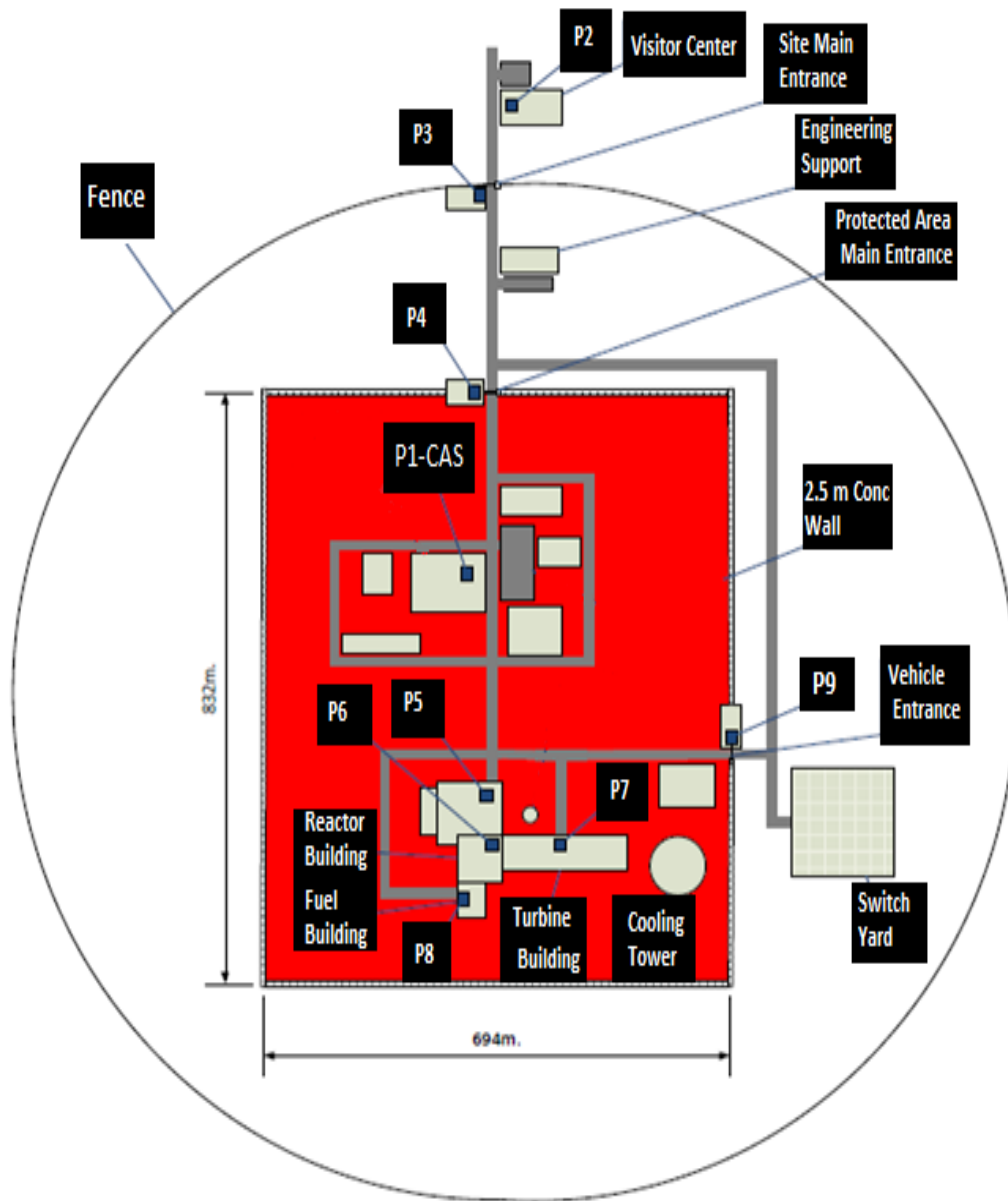
Fig. 5 Hypothetical nuclear reactor facility site diagram
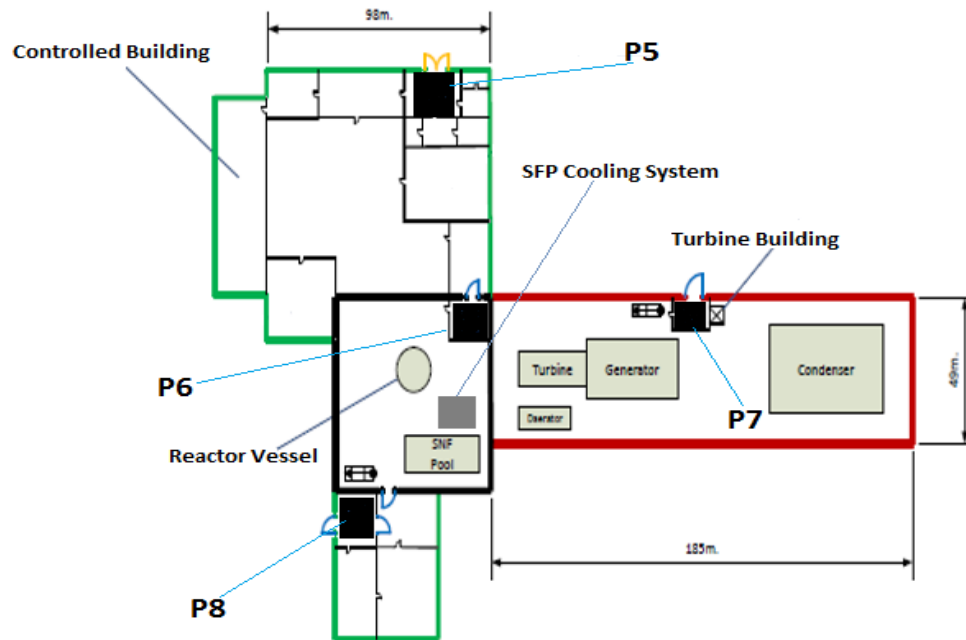
Fig. 6 Hypothetical reactor confinement, with walls and doors (P5, P6, P7 & P8)

2.1.2 Security analysis theoretical principles

The analysis philosophy is to find the risk value of an adversary's specific path. The path has several detection and delay physical protection elements including: patrols, detecting sensor, walls, obstacles, fences, doors, etc., where each protection element has its own detection probability (P_D) and delay time (t_D). As a part of the deployed protection measures, there is a Critical Detection Point (CDP) which is the last detection element, where the response force has enough time to reach the adversaries before they finish their task. The P_I considered as an accumulation of probabilities of detection for each detection element along a path. For calculating of the P_I, we define the non-detecting probability at each detection element to be:

$$B_D{}^j = 1 - P_D{}^j \qquad\qquad (3)$$

Where $P_D{}^j$ is the detection probability at protection element j, so the probability that adversaries will not be defeated (combined non-detection probability) can be calculated by:

$$B_D = \prod_{j=1}^{J} B_D{}^j \qquad\qquad (4)$$

The adversaries might follow several possible paths to reach the target. From the analyst's point of view, the path with the most interest is the path that comes with the combination of the minimum probabilities of interruption and neutralization is the one with highest risk. The worst path for a system may not have lowest P_I, because P_N also contribute as the probability of effectiveness of the security system equal to $P_I * P_N$. After determining the P_I and P_N of the chosen path, this leads to calculating the needed vulnerability value of the chosen path, for the target.

In order to calculate the probability of interruption associated with the chosen path and to evaluate the effectiveness of the deployed PPS, it's necessary to make a scenario of attack and build a scenario graphical model. The graphical model, known as Adversary Sequence Diagram (ASD) views the security system with its detection and delay elements. In order to create an ASD, the following steps have to be applied as following:

- Model the facility by separating into adjacent physical areas.

- Define protection layers and path element at each area.

- Show path segments between the areas through path.

Each protection layers consists of one or more protection elements (the basic building blocks of a PPS). Fig. 7 shows an example of ASD layout and concept:
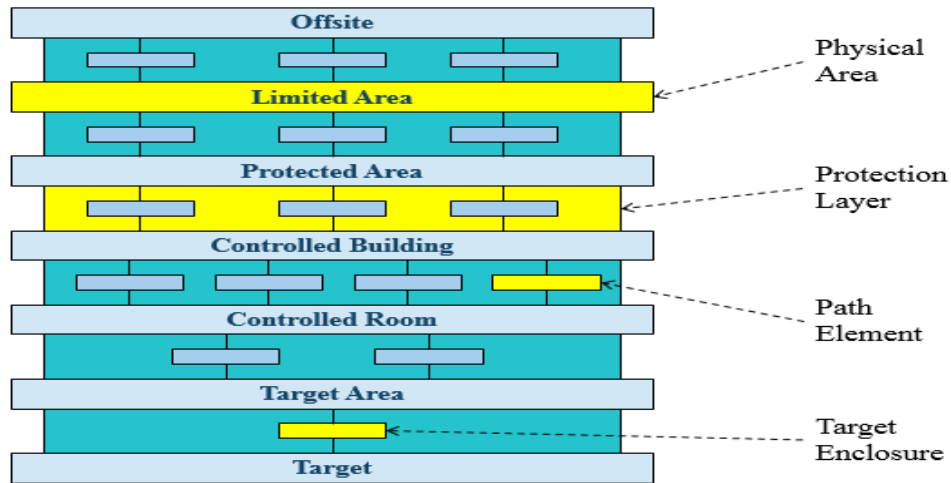
Fig. 7 Adversary sequence diagram layout.

2.2 The Chosen Security Path and Probability of Interruption Calculation

The possible path chosen for this research, which the adversaries might follow is shown in Fig. 8. In this case the adversaries were assumed to conduct a sabotage to the SFP at the reactor building by going through the plant controlled building and reactor building doors respectively (see P5 and P6 in Fig. 6). The adversary's goal is to make severe radiological consequences and contamination to the area either by bombing the SFP that will affect both the spent and fresh fuel, or by bombing SFP cooling equipment which is in the same floor.

21
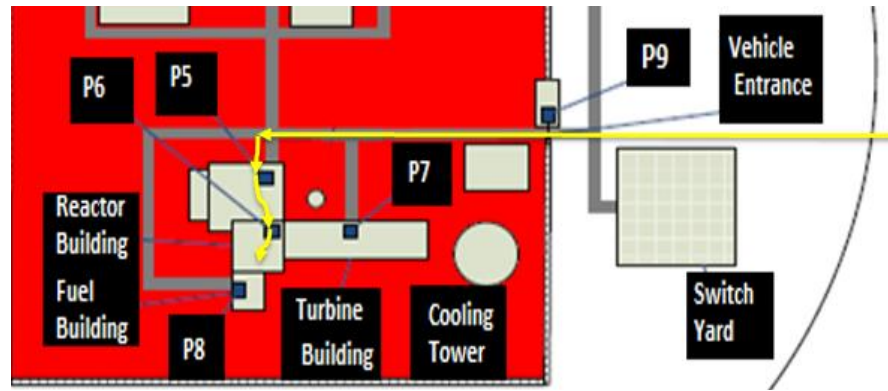
Fig. 8 Probable adversaries attack path

In the previous figure the adversaries moved from the offsite area to the reactor building by penetrating the fence → running to the vehicle door P9 → penetrating the vehicle door → running to the controlled building P5 door → penetrating the P5 door → running to the P6 door → penetrating the P6 door → running to the target → sabotage.

Following the chosen path, the adversary will face several protection layers with protection elements. Assuming the adversary is using explosives to penetrate the doors, the Response Force Time (RFT) was calculated to be 270 seconds with the assumption that the response force will travel by foot and the running speed is 3m/s [20]. Fig. 9 represents the resulting ASD for the chosen security path. Between two physical areas many protection elements are deployed such as vehicle main gate, fence, personnel main gate, walls, and doors where each protection element (such as the 2.5m fence) is represented with two main boxes below. There appear two numbers; the left one represents the detection probability of the protection element as an example the 0.8 P_D of the 2.5m fence, and the right number represents the delay time t_D associated with passing the protection element for example the 10s of the 2.5 fence [20].
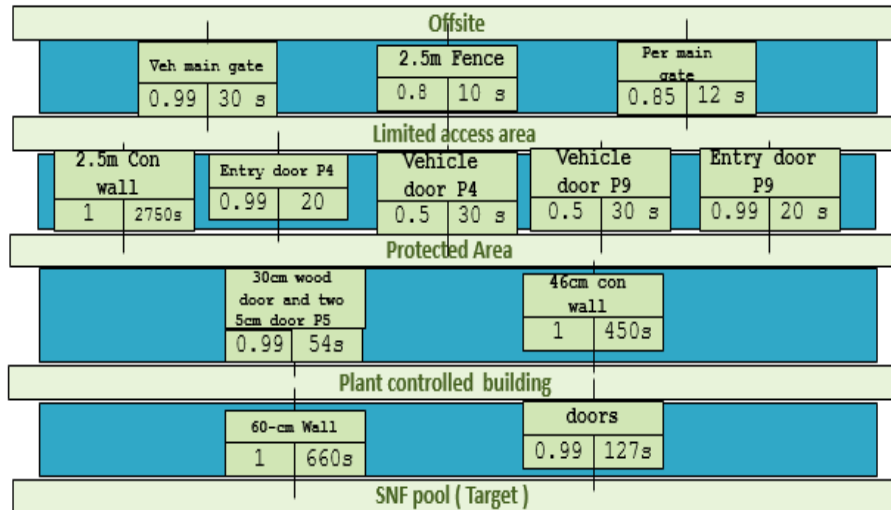
Fig. 9 Controlled building attack path ASD

Based on Fig. 9, the CDP (see subsection 2.1.2) is at the location where the adversaries run to the plant controlled building to penetrate the doors (P5) from the protected area. If they are not detected before completing the penetrating action they are likely to reach the target and sabotage the SFP. As previously mentioned, the EASI model is used for calculating the P_I value, inserting each task's time delay and probability of detection for each layer of the protection element. The probability of alarm communication assumed is 97%, and standard deviation for all time delay is 30% of its value. As an example, the standard deviation is 30% of the response force time, which was calculated to be 270 seconds; therefore the standard deviation is 81 seconds.

Inserting all these parameters and assumptions into the EASI model, which is shown in Table 2, the resulting probability of interruption associated with the chosen path is **0.902**. This is considered a high value of interruption that usually results in a sufficiently low vulnerability in the security system; this also depends upon having a high probability

23

of neutralization by the response force, which depends on the number of the response force members, weapons, training, equipment, and etc. The EASI model includes uncertainty calculation. But for calculating the uncertainty manually, and since it's a multiplication operation, Eq. 5 is used. The P_I error and the B_D error up to the CDP are the same since both terms are related by Eq .3 (see subsection 2.1.2). Table 2 represents the EASI model tasks description and the results of the P_I security sabotage attack calculation.

$$\sigma u = u \sqrt{\left(\frac{\sigma x}{x}\right)^2 + \left(\frac{\sigma y}{y}\right)^2 + \dots} \tag{5}$$

Where σ_u is the error in the term u. While x and y represents the non-detection probabilities (1- P_D) for task 1 and task 2 in Table 2 respectively, and so on up to the CDP (as an example: the non- detection probability of task (1) in Table 2 = 1- P_{D1} = 1- 0.8 = 0.2). In the previous path the CDP is until the third task in Table 2.   With the assumption that the error in each non detection probability is 10%, the non-detection probability error up to the CDP is 0.053.

Therefore, the error in P_I is = 0.054, For the most effective evaluation of the path study, the value of P_I that maximize the vulnerability is considered as the EASI model includes the error and provides the value with the lowest value of P_I. Note: any other manual calculation of the uncertainties is done using the same process as in the previous P_I uncertainty calculation, and by applying the following general uncertainty equation.

$$\sigma^2 u = \left(\frac{\partial u}{\partial x}\right)^2 \sigma^2 x + \left(\frac{\partial u}{\partial y}\right)^2 \sigma^2 y + \left(\frac{\partial u}{\partial z}\right)^2 \sigma^2 z + \dots \tag{6}$$

Where σ_u represents the uncertainty in any value of a math operation.

Table 2 EASI model results of the P_I security sabotage attack calculation

		Probability of Interruption:			0.902
Estimate of		Probability of			
Adversary		Alarm		**System Response**	
				Time (in seconds)	
					Standard
Sequence		Communication		Mean	Deviation
Interruption		0.97		270	81

				Delays (in seconds):	
					Standard
Task	Description	P(Detection)	Location	Mean:	Deviation
1	**Penetrates the Fence**	0.8	e	10	3.0
2	**Run to the vehicle gate at P9**	0.02	P9	90	27.0
3	**Penetrate the vehicle gate**	0.5	P9	30	9.0
4	**Run to the plant controlled building at P5**	0.02	P5	90	27.0
5	**Penetrates the doors at P5**	0.99	P5	54	16.2
6	**Run to the P6 doors**	0.02	P6	20	6.0
7	**Penetrate the P6 doors**	0.99	P6	127	38.1
8	**Run to the SNP pool**	0.02	RB	15	4.5
9	**sabotage the facility**	1	RB	51	15.3

2.3 P_N and Frequency of Attack Calculation

In order to calculate the P_N, the states' competent authority prepares a threat assessment document, which contains information about the anticipated threats such as a terrorist group. This document works as the basis of defining the Design Basis Threat (DBT), which should consist of the attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal of nuclear material or sabotage, against which a nuclear security system is designed and evaluated [21]. The

DBT works as the basis for testing and exercising, making potentially expensive decisions, and the design of nuclear security system.

A major step for estimating the security event frequency is to determine the P_N, which is the result of response force engagement after interruption of the adversaries (P_N can be reduced by adversaries' tactics). For the P_N calculation, the adversaries' capabilities, tactics, and strength are required along with the state's neutralization strategy and measures. Data about the threat, response force, and PPS is required to analyze the engagements and provide the proper value of the P_N. Data about the response force equipment also is needed such as: basic duty weapons, special duty weapons, intermediate force weapons, and vehicles.

Then the neutralization analysis starts by making scenarios and applying analysis methodology. The neutralization analysis method used in this research is a simple numerical method. In addition to this method, other methods can be applied such as: expert opinion, complex computer simulations, simulated physical engagements (Force-on-Force), and actual engagements.

The following assumptions were made on the adversary and response force capabilities. The adversaries are highly trained and have excellent tactics. Their attack plan is at night, and they are a group of 8. They have 7.62 mm semi-automatics, and 9 mm handguns, which are bladed. On the other hand, the response force has four teams of response, which are two armed guards, two men as tactical response, two snipers, and 12 men of offsite response. With these aforementioned assumptions, the P_N value obtained

using an excel macro- calculator (Fig. 4) is **0.94** [19]. Table 3 summarizes DBT for a terrorist group that is considered for the P_N calculation.

Table 3 DBT information for the calculation of the P_N

		Adversary type : Terrorist
Motivation	Ideological	High
	Economic	Low
	Political	High
	Personal	Low
Intentions	Targets of Interest	Sabotage of nuclear or radiological materials
	Likely Malicious Act	Radiological explosion and release onsite and offsite
	Willingness to Die	Yes
Capabilities	Group Size	8
	Tactics	Stealth, Deceit, Speed Assault, Overwhelming Force
	Intelligence Gathering Means	Surveillance from Outside, Passive Insider for Intel, Open Source Analysis
	Weapons	7.62 mm semi-automatic assault rifles, 9 mm handgun, bladed weapon.
	Explosives	Advanced explosives , homemade bombs
	Equipment and Tools	commercially available hand tools and power tools
	Funding	40,000 $
	Modes of Transportation	Light trucks including 4x4, light cars
	Technical Skills	Basic chemistry, basic electronics
	Cyber Skills	No
	Other Knowledge	Yes
	Support Structure	Minor
	Insider Assistance	Yes, passive

Having the P_I and P_N values calculated, and considering the value of the frequency of attack to be 1.0E-03 attack per year [22], the analyst can calculate the frequency of a successful security attack (F_{Se}) using part of Eq .1 as follows:

$$F_{Se} = P_A (1- P_I *P_N) \tag{7}$$

Inserting the previously calculated values into Eq .7 results in $\mathbf{F_{Se}} = \mathbf{1.63\ E\text{-}4}$ successful attack per year. This number considered as the frequency of adversaries' arrival successfully to the target and conducting an attack. This number is used throughout the analysis process in the SAPHIRE.8 code whenever a security attack is presented [14].

2.4 Consequence (C) and Security Risk Estimation

As previously stated the sabotage attack to the SFP might result in a very bad consequence that can lead to the release of a significant amount of radioactivity to the environment. Some examples of damage caused and the consequences of the SFP damage are:

- Mechanical damage to fuel: the direct attack to the SFP might cause damage to the fuel and the release of radioactive materials from the fuel may occur.

- Possible attack by an adversary to the SFP by bombing it could cause direct damage to the pool and leakage of the water from the spent fuel pool, leading to the fuel overheating, resulting in damage to the fuel cladding integrity and the possible release of radioactive materials to the environment.

- Damage to the pool might lead to leakage through the pool liner or evaporation of coolant following the forced loss of the cooling system by targeting it in the attack.

The final parameter that is needed to estimate the security risk value associated with SFP sabotage using Eq .1 is the consequence (C) value. This consequence value can be found using Eq .8.

$$C=0.8*10^{N-7} \tag{8}$$

Where N, is the event level that resulted after failure of system components according to the International Nuclear and radiological Event Scale (INES) [23]. In this analysis, the sabotage of the SFP is assumed to be level 4 accident with a minor off- site release of radioactive materials. The associated relative consequence value C is 8.0E-04. Applying these values to Eq .1 yields the risk value as 1.30E-07 per year for the case of SFP sabotage. The uncertainties in the security analysis calculations can be found in the chapter on results and discussions later.

3. SAFETY ANALYSIS

The SFP components failure analysis was conducted using the PRA level 1 approach, to numerically quantify the risk values, where a series of components failure led to the release of radiation from the pool. In this analysis, the failure frequencies of the cooling system components of the SFP (such as valves, and pumps) were considered to calculate the frequency of failure starting from the basic IE to the whole cooling system failure top event. The purpose of this section is to provide scenarios for cooling system failure along with the calculation of the frequency of failure associated with each analyzed scenario. Three scenarios were analyzed (subsection 3.3) as follows:

- All natural mechanical failure of the SFP cooling system.

- Heavy load drop external IE accompanied with natural failure.

- Seismic external IE accompanied with natural failure.

The first step in a PRA is to identify a top event and different IE's that could lead to this event. For this reason, fault trees are used to identify and quantify possible system failures. At the lowest level of the fault tree is the basic event assigned with a frequency value. The frequency used is a value representing how many times an event likely to happen during a time frame (ex. 1/year). Each event in the fault tree has its frequency value, where the Boolean logic is followed to determine the frequency of failure of the top event. In order to calculate the top event frequency of failure, each individual component failure frequency must be found first. The initial frequency of failure data includes the

30

number of incidents and associated observation time (taking into account the fraction of time the plant is operational). The sources for this data could be:

- Plant specific data: data derived from information directly collected at the plant.

- Generic data: data derived from information not associated with the plant being analyzed, might be from similar plants or similar components used at other plants [24].

A lack of observation of the hazardous events might create difficulties in estimating the frequency of these events. In this case, the generic data method was used instead to provide a frequency data of events. In this research, the data for the cooling system components of the SFP is generic data, since the SFP layout is a hypothetical one. As mentioned before, the basic event is the lowest level of a fault tree, representing an IE. An IE is an event that creates a disturbance in the plant and has the potential to lead to complete system damage [25], such as:

- Internal events occurring during operation. (Such as failure of plant equipment, human errors, and loss of off-site power).

- Internal hazards (internal fires, internal floods, and missiles).

- Transients.

- Loss of Coolant Accidents (LOCAs)

- External hazards (Natural, Human made such as Security events).

Each cooling system component such as pumps and valves has its own failure frequency [26]. The main pumps in the primary and the secondary cooling system (see

31

Fig. 2) have a natural random mechanical failure frequency of **3.00E-05** per year. Likewise, the valve's failure frequency is **1.3E-02** per year [27].

3.1 Probabilistic Safety Assessment and Evaluation

There is no safety without safety assessment, which is a systematic process that is carried out throughout the life time of the facility or the activity to ensure that the relevant safety requirements are met by the proposed or actual design [28]. The design of nuclear safety systems must be able to fulfill their function in an adequate manner, even in the event of failure of any one of their components. To ensure that the deployed safety systems meet the facility independency, diversity, and redundancy safety standards, at least two safety systems with the exact same function are generally installed. Fig. 10 shows an example of implementing the previously mentioned safety standards for the SFP cooling system in a reactor. For example, in this figure there are two cooling system heat exchangers (independency) each with its pump, which is driven by a different type of electricity source (diversity), and two separate operation pipes. Only one of each duplicate element is needed at a time (redundancy).
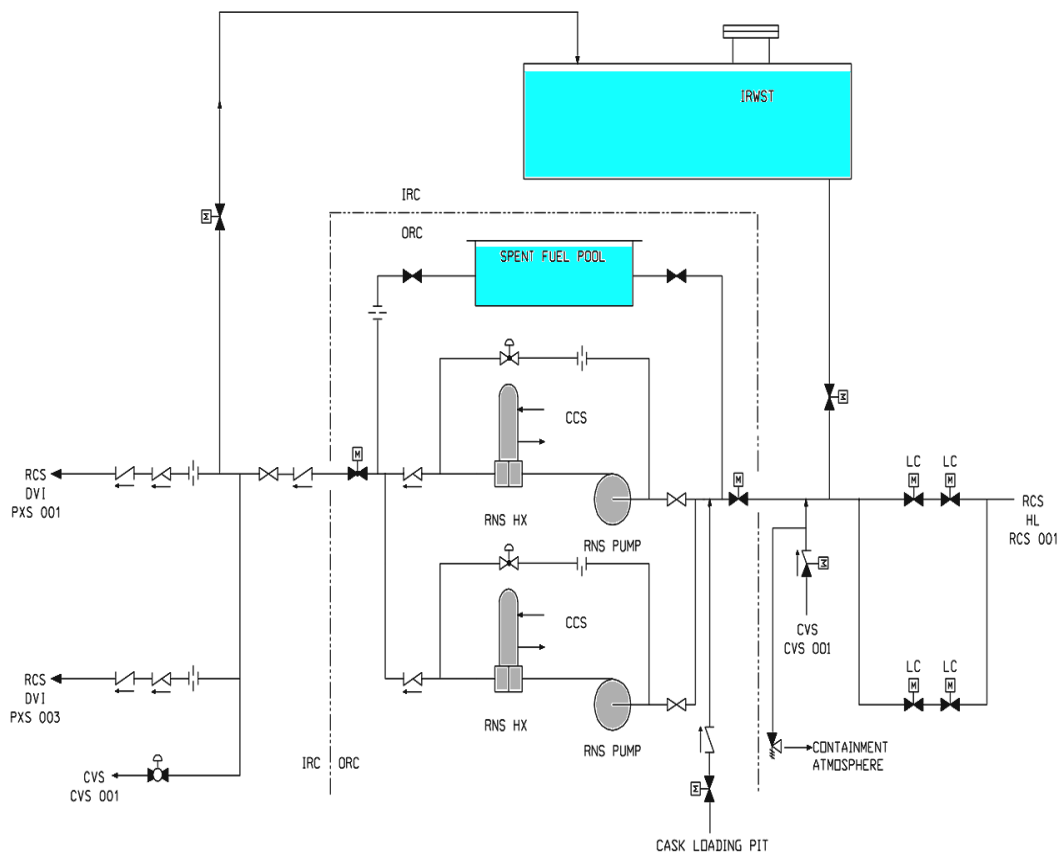
Fig. 10 An example of SFP cooling system safety standards [30]

The steps of the probabilistic safety assessment are summarized as follows:

- Selection of the external event (Hazard).

- Hazard assessment.

- Analysis of the response.

- Model development.

- Risk quantification and interpretation of results.

- Measures development and implementation to reduce high risk.

33

As the frequency of an event increases, the severity (consequence) of this event increase as well, which in turn push the decision maker to modify the existing systems to reduce the risk value. In other words, the purpose of the risk assessment in nuclear safety is to evaluate the risk upon which the decision-making process depends. Fig. 11 shows the relation between the frequency of an event and the consequence severity. In order to estimate the severity of an event, sources of risk must be identified and accounted for. Risk can be caused by a natural disaster (such as in the case of Fukushima nuclear power plant) or can be a side effect of human error (such as in the case of Chernobyl nuclear power plant).
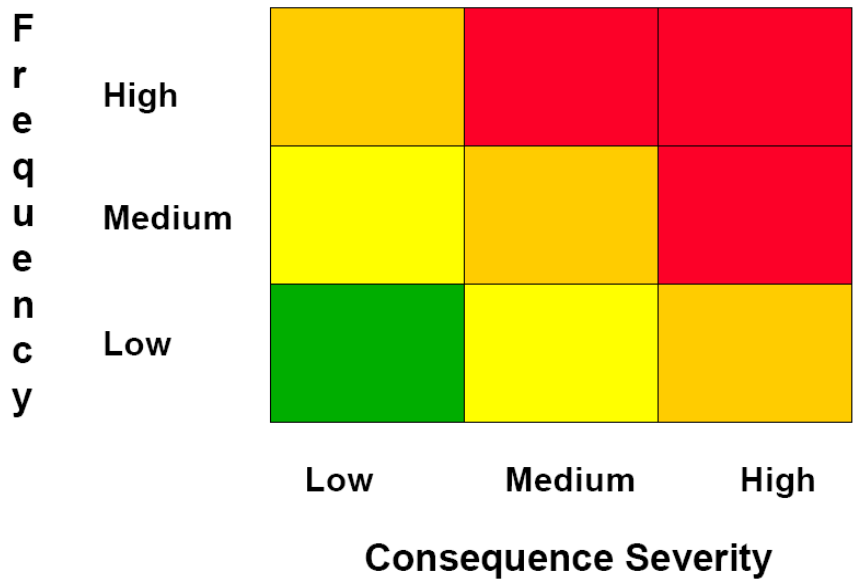
Fig. 11 Frequency level vs consequence severity [29]

3.2 The Boolean Analysis Method

This section provides a brief explanation about the Boolean logic method, which was used in calculating the top event frequency starting from basic event. The Boolean method helps trace a series of events that could lead to the top event. The series of events start with an IE and then could progress to a top event, which are chains of events that link the initiator to the top event. The Boolean logic method has indicator names and operators as follows:

- Indicator names: True, 1, Yes, False, 0, and No.

- Main Boolean operators, also called gates, are:

    - OR (represents addition, otherwise symbolized as +),

    - AND (represents multiplication, otherwise symbolized as * or x).

    - NOT (represents symbols such as /, /x, x', ').

Developing failure scenarios starts with making fault trees (a deductive analysis that allows analysts to proceed from the top event to elementary events) to graphically represent the interaction of a component failure and other events within a system using the Boolean logic method [30]. Fig. 12 below shows an example of how to graphically represent the component failure in a specific system as a fault tree, starting from the basic event that may lead to the system failure. The fault tree allows identifying sequences (or combinations) of events that result in system failure. The combination of events are described by the logical AND and OR (and occasionally NOT) Boolean operators.

35
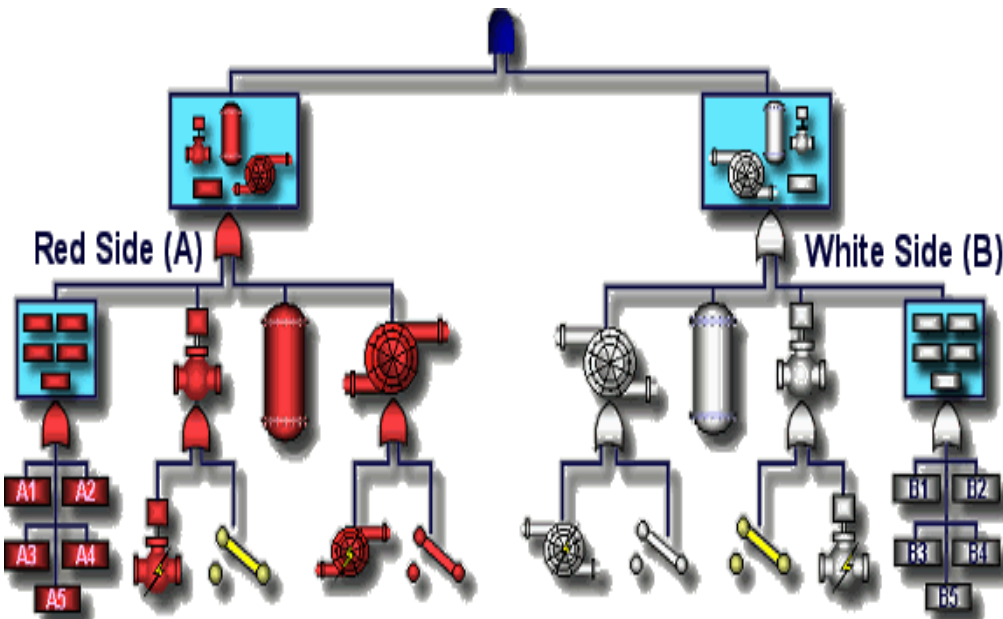
Fig. 12 Components failure fault tree graphical representation [29]

Fig. 13 provides an example of a hypothetical situation for a top event (T) representation initiated by the basic events A, B, or C. [29]. The failure of top event (T) is conditioned by the failure of (C) or failure of both (A&B). If the individual frequency of each of the basic events (A), (B,) and (C) is known, the top event frequency (T) can be calculated by substituting the frequency values of (A), (B), and (C) in (T=C+A*B). To verify how (T= C+A*B), Boolean logic method is implemented, starting from the top of the fault tree in Fig. 13 and moving down as following:
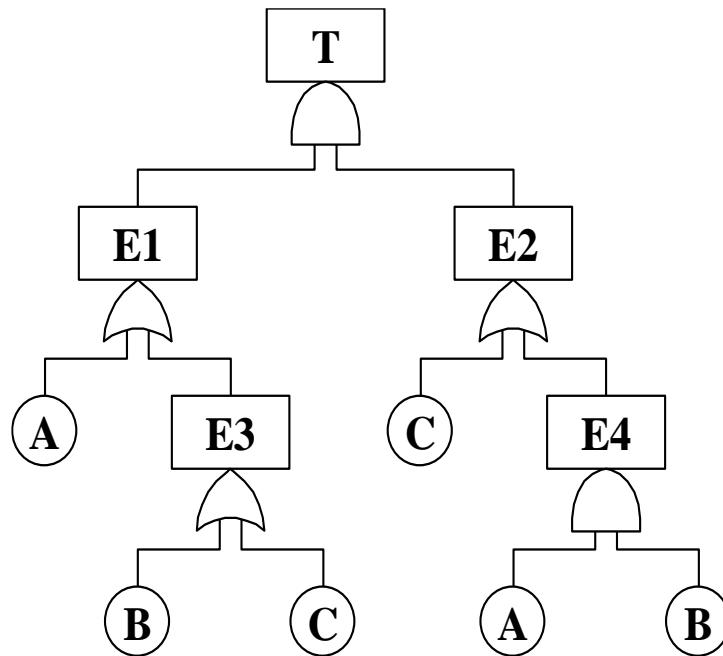
Fig. 13 Fault Tree of Top event (T) initiated by basic events A, B, or C

T= E1*E2, (Since an AND gate is between E1 and E2).

E1= A+E3 (since an OR gate is between A and E3).

E2= C+E4 (since an OR gate is between C and E4).

Then substituting the values of E1 and E2 in T

T= (A+E3)*(C+E4) = (A*C) + (A*E4) + (E3*C) + (E3*E4).

 E3=B+C.

 Substituting in T

T= A*C+A*E4+ (B+C)*C+ (B+C)*E4

T = (A*C+B*C+C*C+E4*C) +A*E4+B*E4

T=C+A*E4+B*E4, where E4=A*B.

T=C+A*A*B+A*B*B.   Applying some Boolean algebra rules (such as: A*A= A, A+A=A, A*(A+B) = A), then T will be:

T=C+A*B

Most of the fault trees that were built in this research were direct and simple fault trees. Fig. 14 shows an example that illustrates how to calculate the frequency of top event from a combination of basic events for such a simple fault tree.
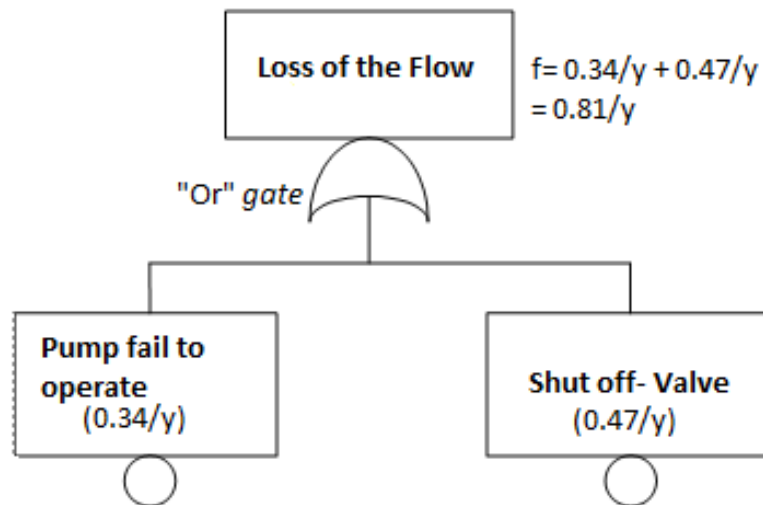
Fig. 14 Top event frequency calculation example.

After calculating the frequency of the top events, the next step is to evaluate the consequence for risk value estimation. In this study, this evaluation was performed using an event tree (see Fig. 15), which is a graphical technique to evaluate the consequence by mapping all probable outcomes of an IE in logical sequence [31]. An event tree is generated by combining the top events as functions. These functions are represented as

blocks with two arrows, either success (upward arrow) or failure (downward arrow). The following steps summarize the event tree representation process:

- Determination of possible plant responses to each of the IE

- Identification of the event sequences that could occur following success or failure of system function.

- Categorise the event sequences identified as success (ex. safety functions satisfied) or failure (ex. fuel damage)
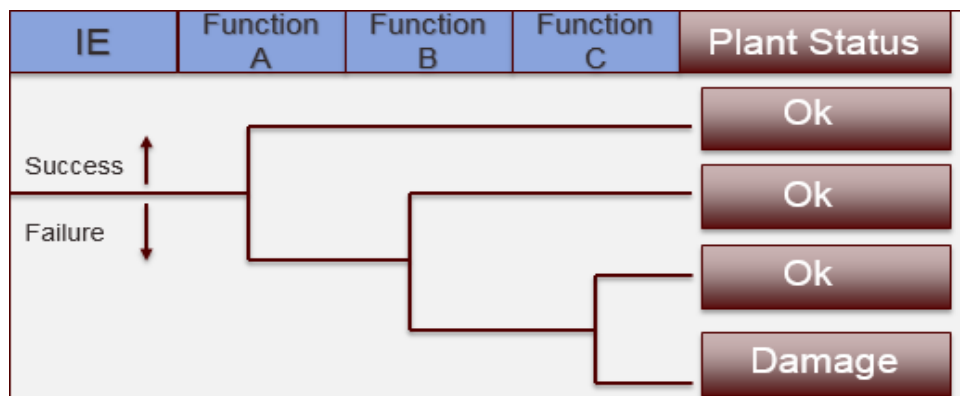
Fig. 15 Event tree representation example

After an IE triggers an accident sequence (a chain of events linking the initiator and possible consequences), the outcome depends on the success or failure of the built-in safety functions; the worst case scenario might be reached if a specific function or several functions fail. Fig. 16 shows an example of an event tree accident sequence representation, the functions blocks represents safety and security systems with a security attack as an IE.

In this figure the failure of functions C, D, and E leads to an undesirable consequence (for example, fuel damage in a nuclear facility fuel storage area).
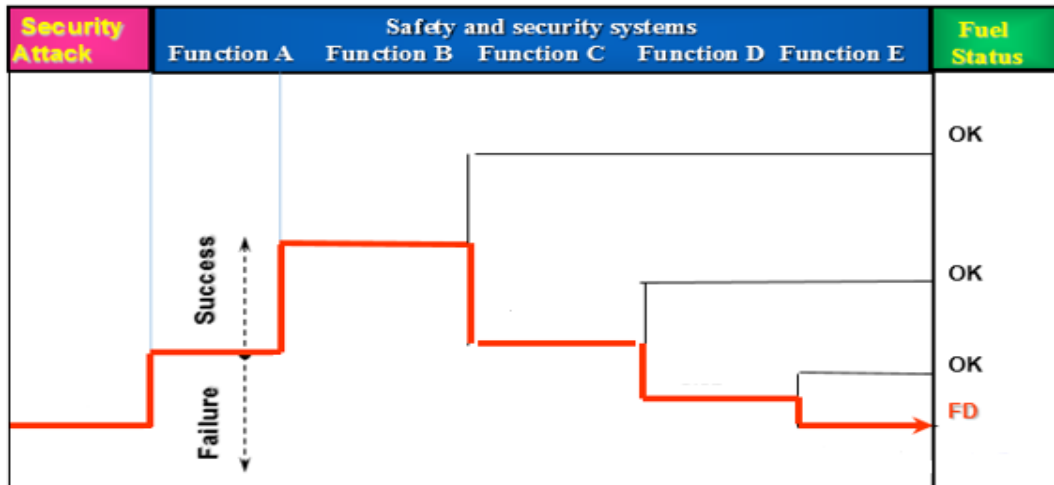
Fig. 16 Accident sequence representation of an event tree.

3.3. Safety Failure Analysis of the SFP Cooling Systems

This section reports the analysis that was conducted on the SFP cooling system to find the combined failure frequency of the primary and secondary cooling systems (see Fig. 2 for the layout of the cooling system) by building fault trees using SAPHIRE software. Also a natural failure of either primary or secondary cooling systems combined with a failure due to a natural external event was considered. As mentioned before the primary cooling system provides the main cooling requirements to the SFP during normal conditions, while the secondary cooling system provides cooling during abnormal and

accident conditions. The following subsections provide several failure scenarios with the failure frequency calculations.

3.3.1. Natural failure frequency calculation of the primary and secondary cooling systems independently

The main components of the primary cooling system that can cause a failure to the system are: the main valve, valve-1, valve-2, pump-1, and pump-2. Primary cooling system failure can be occur due to the natural failure of any of the following:

- Main cooling pumps 1 and 2 simultaneously.

- The main valve.

- Valves 1 and 2

- Valve-1 and main pump-2

- Valve-2 and main pump-1

A fault tree that is constructed for the primary cooling system of the SFP is shown in Fig. 17. The numbers in Fig. 17 represent the individual component (pumps, valves) failure frequency. Fault tree analysis provided the total natural random frequency of failure of the primary cooling system as **1.31E-02** per year (by applying Boolean logic method, which was discussed in section 3.2).

41
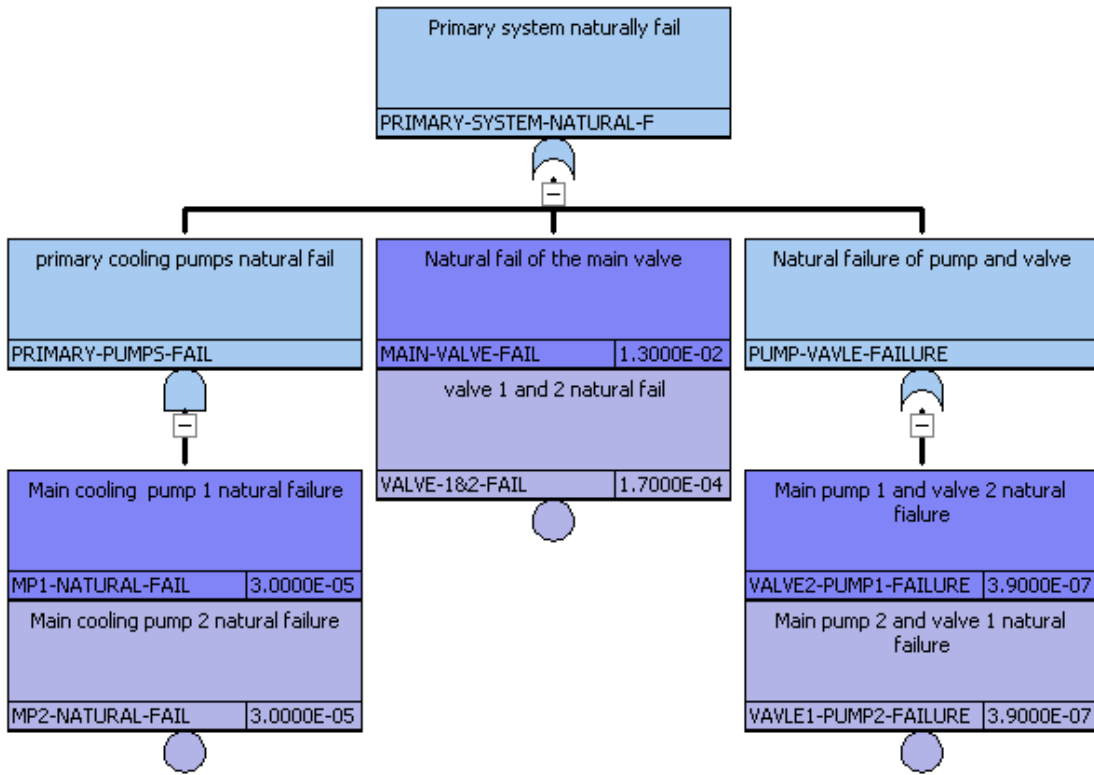
Fig. 17 Primary cooling system natural failure fault tree

The secondary cooling system has two main components, which are the two cooling pumps. Failure of the secondary cooling system occurs when the electrical driven cooling pump and the diesel driven cooling pump fail simultaneously. Each pump has a failure frequency of **3.00E-5** per year. The fault tree that is constructed for the secondary cooling system of the SFP is shown in Fig. 18. The numbers in Fig. 18 represent the pumps' failure frequency. The fault tree analysis provided the overall natural random failure frequency of the secondary cooling system as **9.00E-10** per year.
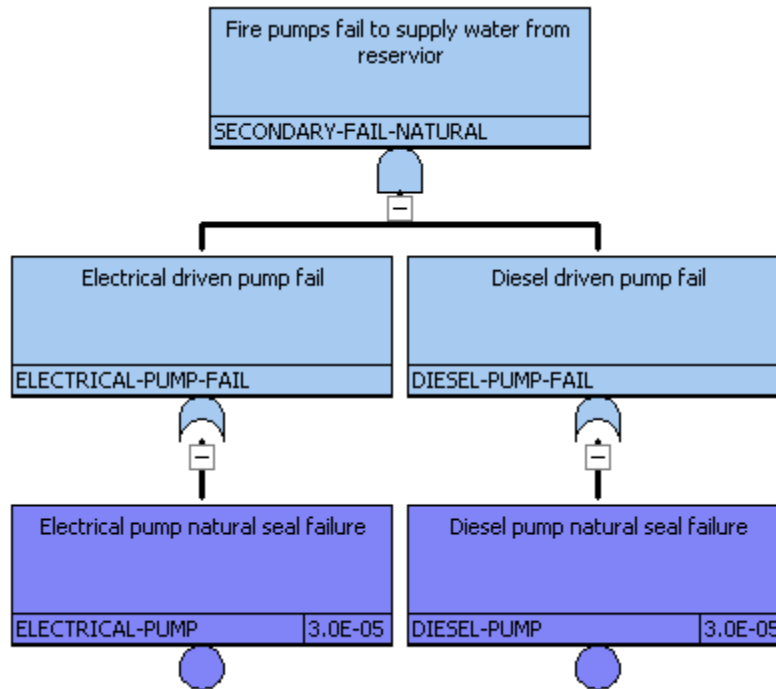
Fig. 18 Secondary cooling system natural failure fault tree

3.3.2. *The simultaneous natural failure frequency of the primary and secondary cooling systems*

The primary and secondary cooling systems might simultaneously fail naturally as described in the event tree shown in Fig. 19. In this scenario, the total frequency of failure for the cooling systems is: the natural frequency of failure for the primary cooling system 1.31E-02 per year (see Fig. 17) times the natural frequency of failure for the secondary cooling system 9.00E-10 per year (see Fig. 18) which is equal to **1.18E-11** per year. This frequency value is the SFP cooling system natural safety frequency of failure.

43
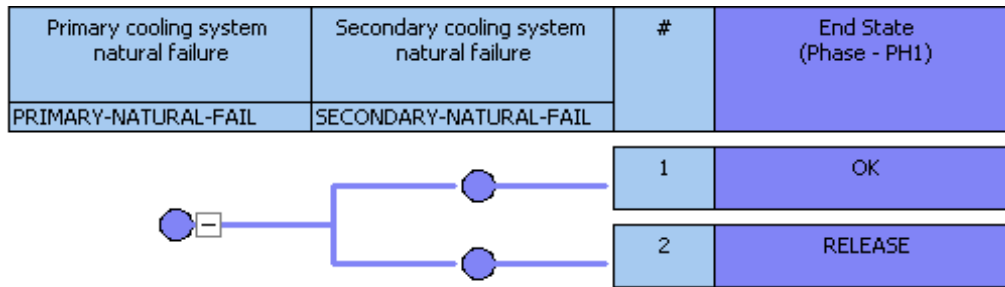
Fig. 19 Primary and secondary cooling systems natural failure event tree

3.3.3. *Natural failure frequency of the SFP cooling system initiated by a heavy load drop*

In this analysis, the failure of the cooling system occurs due to the failure of both primary and secondary cooling systems simultaneously, initiated by an external or internal event and a natural mechanical component failure. Many scenarios could be analyzed such as a heavy load dropped on the primary cooling system causing it to fail, accompanied by natural failure of the secondary cooling system. The event tree in Fig. 20 represents this scenario.

To calculate the total frequency of failure for this scenario, the heavy load drop frequency is needed, which is equal to **2.1E-05** per year [13]. Then, the total frequency of failure is: the frequency of failure for the primary cooling system due to the heavy load drop (2.1E-05 per year) times the natural frequency of failure for the secondary cooling system (9.00E-10 per year), which is equal to **1.89E-14** per year.

Another scenario was considered, in which the cooling system failure is due to a heavy load dropped on the secondary cooling system causing it to fail accompanied by a

44

simultaneous natural failure of the primary cooling system. This is unrealistic scenario to happen, but still a scenario to be analyzed. Fig. 21 represents this scenario. Then, the total frequency of this type of failure is: the natural frequency of failure for the primary cooling system(1.31E-02 per year) times the frequency of failure for the secondary cooling system due to heavy load drop (2.1E-05 per year),which is equal to **2.75E-07** per year.

Primary cooling system failure due to heavy drop	Secondary cooling system natural failure due to pupms fail	#	End State (Phase - PH1)
PRIMARY-HEAVYDROP-FAIL	SECONDARY-NATURAL-FAIL		
		1	OK
		2	RELEASE
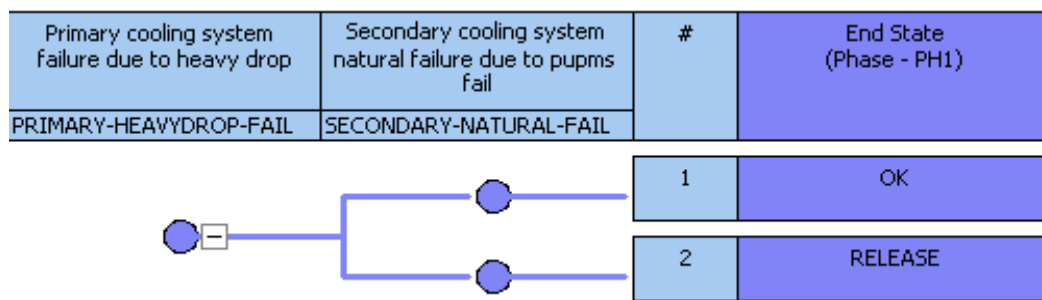
Fig. 20 Cooling system failure due to heavy load drop with natural failure

Primary cooling system natural failure	Secondary cooling system failure due to heavy load drop	#	End State (Phase - PH1)
PRIMARY-NATURAL-FAIL	SECONDARY-HEAVYDROP-FAIL		
		1	OK
		2	RELEASE
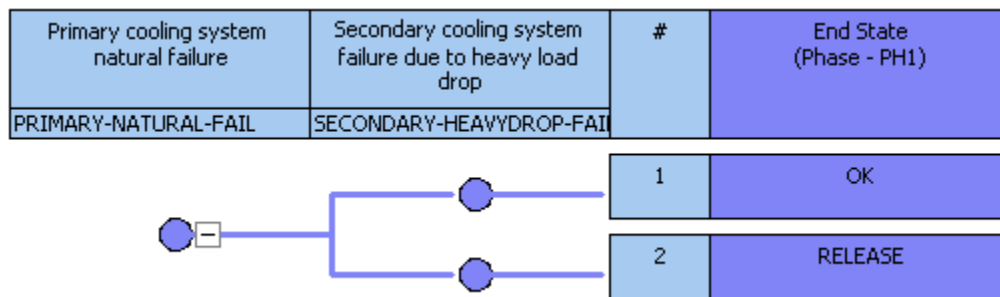
Fig. 21 Cooling system failure due to natural failure with heavy load drop

45

3.3.4. Natural safety failure frequency of the SFP cooling system initiated by a seismic event

In this section, two scenarios are analyzed. First the primary cooling system fails to operate due to a seismic event, accompanied by natural failure of the secondary cooling system. The event tree in Fig. 22 represents this scenario. The seismic event frequency is **2.0E-6** per year [13]. Therefore, the total failure frequency of the cooling system in this scenario is: the frequency of failure for the primary cooling system due to seismic event (2.0E-06 per year) times the natural frequency of failure for the secondary cooling system (9.00E-10 per year) which is equal to **1.80E-15** per year.

The second scenario is that a natural failure of the primary cooling system, accompanied by a seismic event causes the secondary cooling system to fail. The event tree represents this scenario shown in Fig. 23. The total frequency of failure for the cooling system is: the natural frequency of failure for the primary cooling system (1.31E-02 per year) times the secondary cooling system failure due to a seismic event (2.0E-06 per year), which is equal to **2.62E-08** per year.
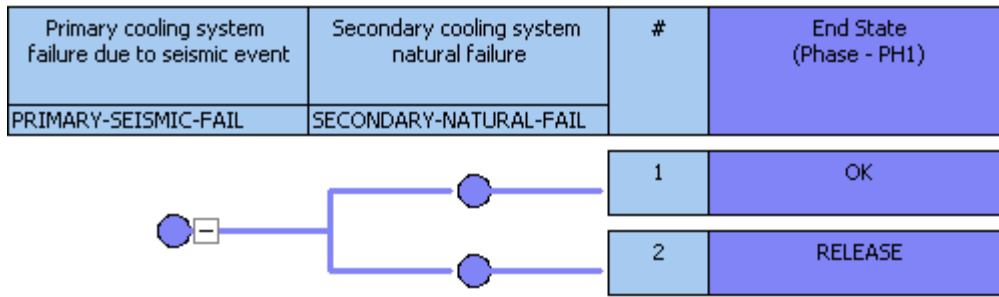
Fig. 22 Cooling system failure due to seismic with natural failure
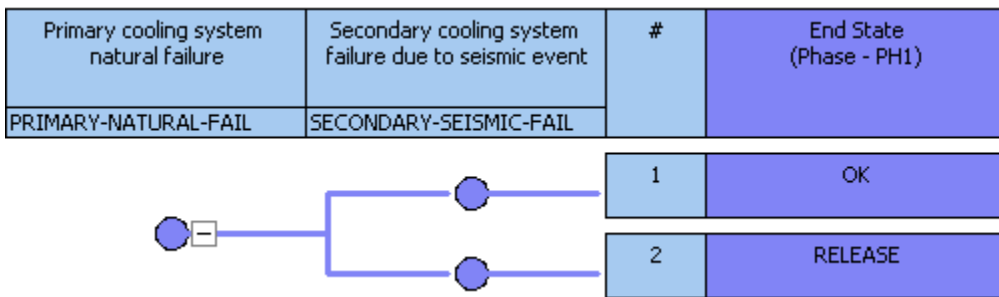
Fig. 23 Cooling system failure due to natural failure with seismic

3.4. Safety Cooling System Natural Failure Risk Estimation

Calculation of the risk value requires knowledge of the consequence value (C, in Eq.1 and Eq.2). Using Eq .7 with a level 4 accident on the INES scale, the associated consequence value C is 8.0E-4. The risk value associated with each scenario of failure is estimated by multiplying the consequence value with the failure frequency using Eq .2. Table 4 summarizes the previously calculated failure frequencies and gives the risk estimates of each natural safety failure scenario described in section 3.3., also the security initiated failure frequency values.

Table 4 Failure frequencies and risk values for the SFP cooling system failure scenarios (safety and security without overlap)

Scenario No.	Scenario Description	IE Failure Frequency/ y	Total Failure Frequency/ y	Risk / y
1.	All natural safety failure	1.31E-02	1.18E-11	9.44E-15
2.	Heavy load dropped on the primary system and natural failure of the secondary system	2.1E-05	1.89E-14	1.51E-17
3.	Natural failure of the primary system and heavy load dropped on the secondary system and	1.31E-2	2.75E-07	2.20E-10
4.	Seismic event on the primary system and natural failure of the secondary system	2.0E-06	1.80E-15	1.44E-18
5.	Natural failure of the primary system and seismic event on the secondary system and	1.31E-02	2.62E-08	2.09E-11
6.	**All security failure**	**1.0E-03**	**1.0E-03**	**1.52E-07**

4. SAFETY- SECURITY SYSTEMS COMBINED ANALYSIS

This section introduces the combined safety-security failure analysis process for the cooling system of the SFP target. The results of a combination of component failures based on a specific scenario were analyzed to determine the main system failure frequency. Several IE's can trigger serial system failure. This could be security IE followed by a safety system failure or started by natural failure followed by a security event. The joint safety-security analysis of the SFP cooling system failure is carried out by forming event trees accounting for component failure scenarios with a security event. For quantitative assessment of risk associated with system failure frequency, many IEs categories were considered in analyzing the system failure process such as:

- Security event

- Heavy load drop event

- Seismic event

- Tornado

- Aircraft impact

- Internal Fire

- Loss of coolant inventory

The previous section discussed only two examples of IE, but this section extended into more IEs to show the range of possible IEs that the analyst usually should consider in

the analysis process. Considering more IEs should contribute to a more comprehensive total risk value estimation.

In order to calculate the total frequency of failure of the SFP cooling system, the frequency of IE needs to be known. The frequency of a security IE was estimated in security analysis section-2 earlier in this research to be 1.63E-04 per year, in which this frequency value was determined based on the probability of adversaries' attack and the vulnerability of the security systems. As previously mentioned the heavy load drop frequency is 2.1E-05 per year while the seismic IE frequency is 2.0E-6 per year [13].

A security based terrorist attack could compromise the objectives of the SFP cooling system by causing it to drain completely or partially resulting in numerous negative consequences. Once the water level in the pool falls down, the level of radiation increases, which could prevent direct safe access to the area around the SFP building. Also the ability to remove the decay heat would be reduced especially when the water level drops much below the top of the fuel assemblies. This would increase the temperature of the fuel assemblies, and might cause oxidation of the zirconium cladding. Also this could cause a fuel meltdown and large amount of radioactive material release, which is the main goal of the adversaries. The next section explains the analysis of the combined failure scenario with the calculation of the joint failure frequencies.

4.1. Combined Safety-Security Failure Frequency of the Cooling System

Many scenarios could be analyzed based on the behavior of the adversaries once they arrive at the SFP area, as they might bomb the pool itself or its components. Each action the adversaries might take is considered as an IE. Fig. 24 shows the event tree of both the adversaries' possible attacks and cooling system components' natural failure. These adversaries' possible attack include: Direct attack to the spent fuel pool, attack to the primary cooling system, or attack to the secondary cooling system.

Combining the attack scenario at the primary cooling system with the natural failure process would change the primary cooling system natural failure fault tree (see Fig. 17) to as it appear in Fig. 25. According to SAPHIRE.8 software, the new calculated combined failure frequency of the primary cooling system is **1.31E-2** per year, which is the same as the natural frequency of failure of the primary cooling system since the valve failure frequency (1.30E-02 per year) dominates the failure process. Fig. 26 shows the fault tree of the secondary cooling system failure including a security attack. The next sections present the failure scenarios for the cooling system due to security sabotage accompanied by natural safety failure or external events such as: (1) heavy load drop (2) seismic event (3) tornado (4) aircraft crash.

Adversary successfuly arrive the SFP area	Adversary bomb the SFP	The adversary bomb the primary cooling pumps	Secondary cooling system naturally fail	The adversary bomb the secondary cooling pumps	Primary cooling system naturally fail	#	End State (Phase - PH1)
ADVERSARIES-ATTACK	SFP-BOMBING	PRIMARY-BOMBING	SECONDARY-FAIL	SECONDARY-BOMBING	PRIMARY-FAIL		
						1	OK
						2	OK
						3	OK
						4	RELEASE
						5	RELEASE
						6	RELEASE
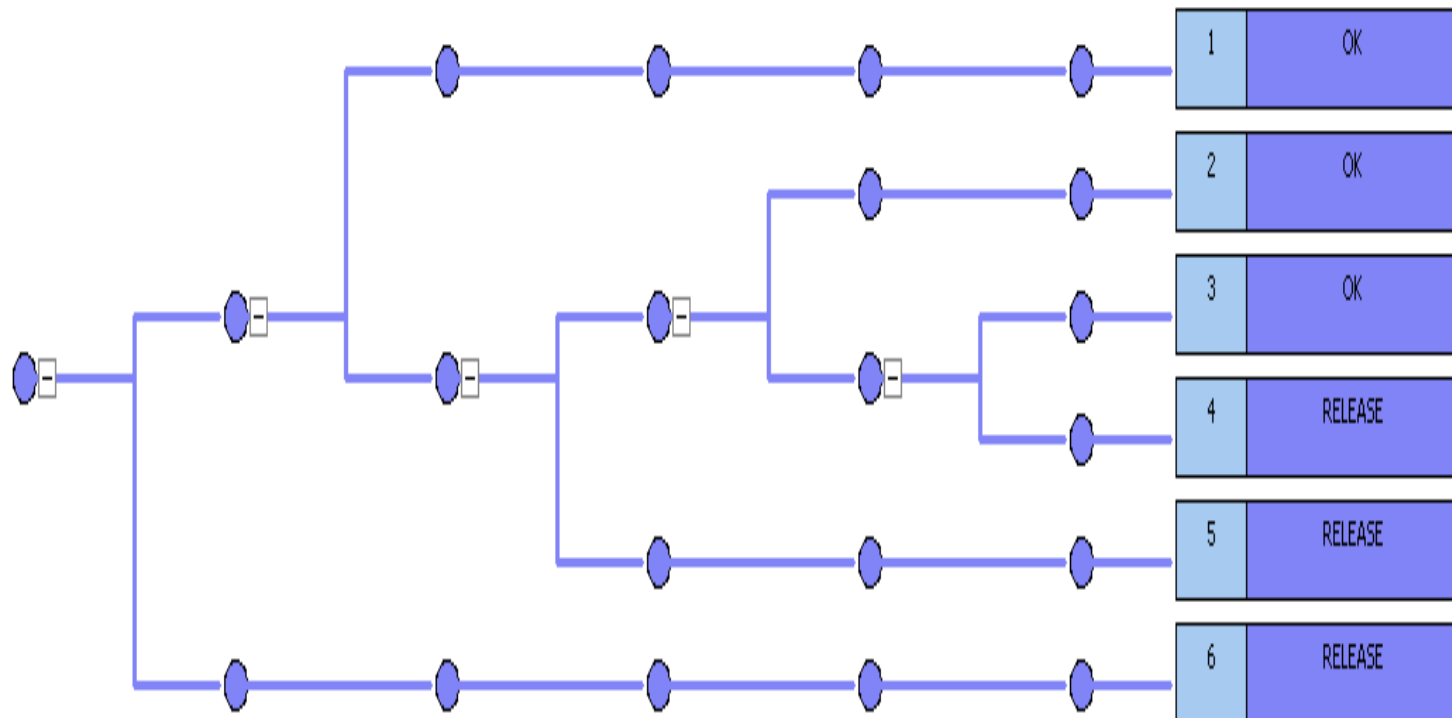
Fig. 24 Event tree of possible SFP failure scenarios including security attack
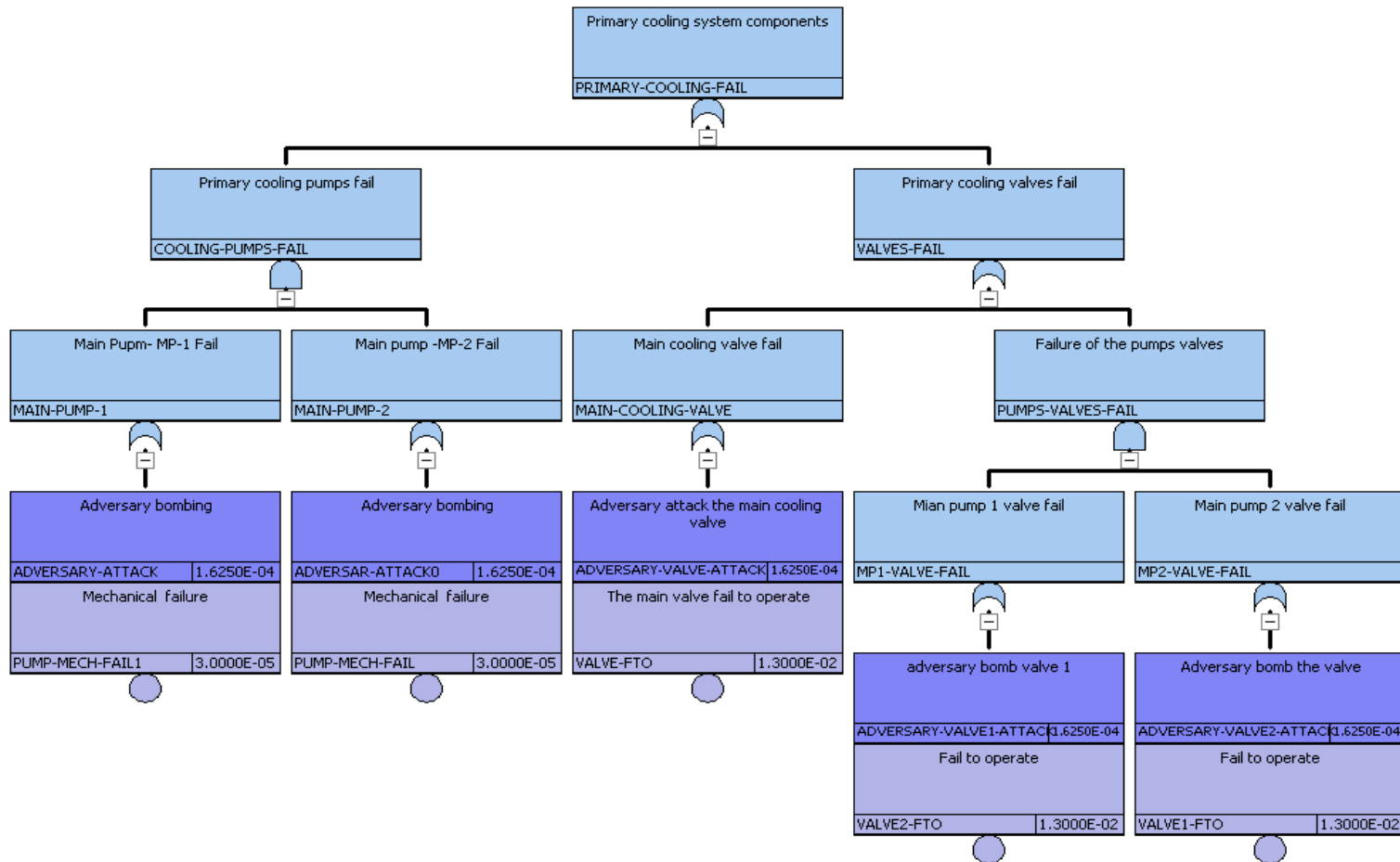
Fig. 25 Fault tree of primary cooling system failure including security attack
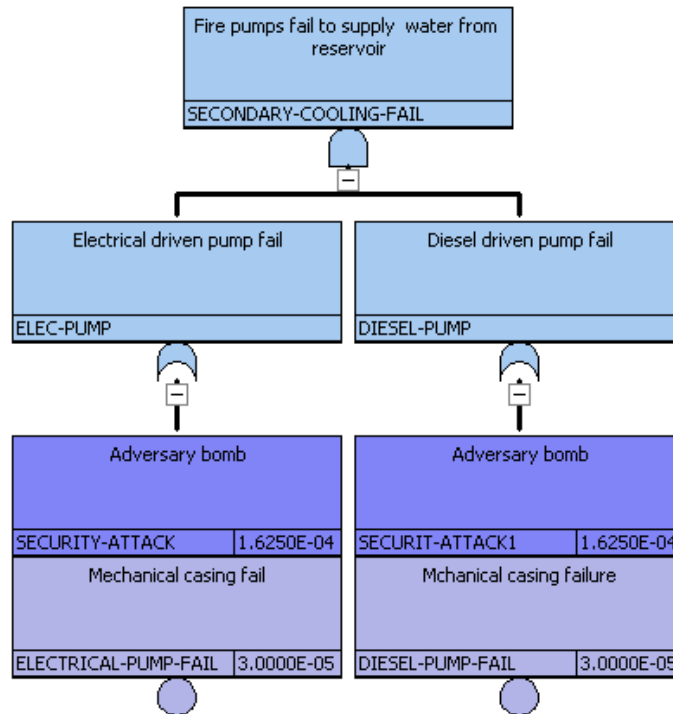
Fig. 26 Fault tree of secondary cooling system failure including security attack

4.1.1. Security sabotage of the primary cooling system and natural failure of the secondary cooling system

This failure scenario included a security sabotage event at the primary cooling system in conjunction with a natural failure event at the secondary cooling system. The event tree constructed for this scenario is shown in Fig. 27. The objectives of the scenario analysis for a security sabotage event are (1) to calculate the joint frequency of failure and risk value in order to compare these values to the resulting values of a cooling system failure without a security event, and (2) to determine how much a security event can affect the risk value.

54

The joint failure frequency is determined by combining the security attack frequency at the primary cooling system, which is 1.63E-04 per year (see section 2.3) with the secondary cooling system natural failure frequency (9.00E-10 per year) , which is **1.47E-13** per year.

Primary cooling system failure due to security attack	Secondary cooling system natural failure	#	End State (Phase - PH1)
PRIMARY-SECURITY-FAIL	SECONDARY-NATURAL-FAIL		
		1	OK
		2	RELEASE
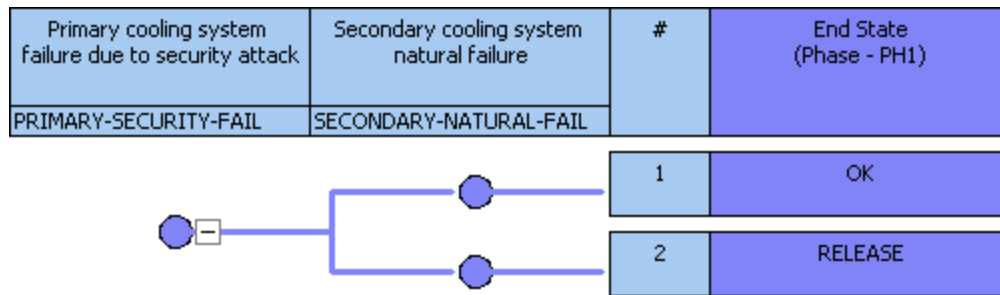
Fig. 27 Cooling system failure scenario due to security attack with natural failure

4.1.2. Natural failure of the primary cooling system and security sabotage of the secondary cooling system

The joint failure frequency calculation for this scenario is found by combining the natural failure frequency at the primary cooling system (1.31E-02 per year) with the secondary cooling system failure due to security sabotage (1.63E-04 per year) which is **2.14E-06** per year. The event tree constructed for this scenario is shown in Fig. 28.
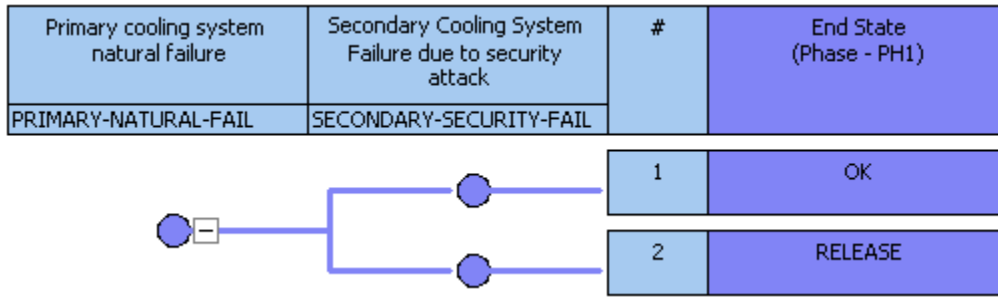
Fig. 28 Cooling system failure due to natural failure with security attack

4.1.3. Cooling system failure due to security sabotage in conjunction with a heavy load drop event

If any attack causes the primary cooling system to fail, the secondary cooling system will be triggered to start injecting water to the pool. This scenario analyses a security sabotage attack caused failure at the primary cooling system accompanied by failure of the secondary cooling system due to heavy load drop. The event tree below in Fig. 29 shows the failure process of this scenario.

Fig. 29 Cooling system failure due to security attack with heavy load drop

The joint frequency of failure calculation is found by combining the security attack frequency at the primary cooling system (1.63E-04 per year) with the heavy load drop frequency at the secondary cooling system (2.1E-05 per year) which is **3.42E-09** per year. Note: if the scenario were changed as the security attack happening at the secondary cooling system with heavy load drops at the primary cooling system, this gives the same joint failure frequency value (because the security attack event and the heavy load drop event have fixed frequency values).

4.1.4. Cooling system failure due to security sabotage in conjunction with a seismic event

This failure scenario includes a security sabotage event in conjunction with a seismic event that caused failure to either the primary or secondary cooling systems. In this scenario, a security sabotage attack caused failure at the primary cooling system accompanied by failure of the secondary cooling system due to seismic event. This scenario is unrealistic to happen, but still could be analyzed. The event tree constructed for this scenario is shown in Fig. 30.
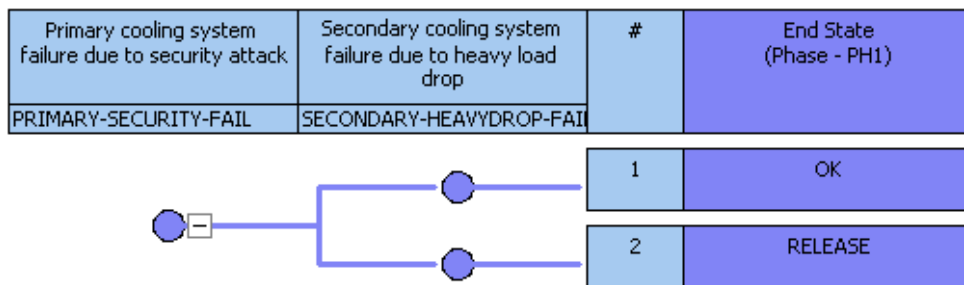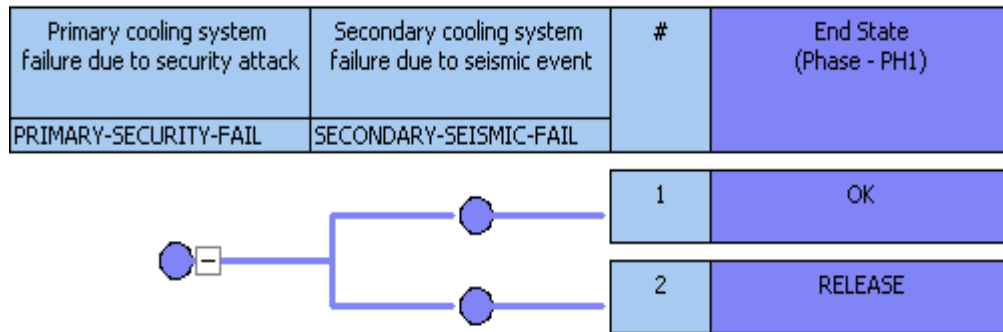
Fig. 30 Cooling system failure due to security attack with seismic

The joint frequency of failure calculation is found by combining the security attack frequency at the primary cooling system (1.63E-04 per year) with the seismic event frequency at the secondary cooling system (2.00E-06 per year), which is **3.28E-10** per year. Note: if to change the scenario as the security attack happening at the secondary cooling system with seismic event at the primary cooling system, this gives the same joint failure frequency value (because the security attack event and the seismic event have fixed frequency values).

4.1.5. Cooling system failure due to security sabotage in conjunction with a tornado

In this scenario, a security sabotage attack caused failure at the primary cooling system accompanied by failure of the secondary cooling system due to a tornado is analyzed. The event tree constructed for this scenario is shown in Fig. 31
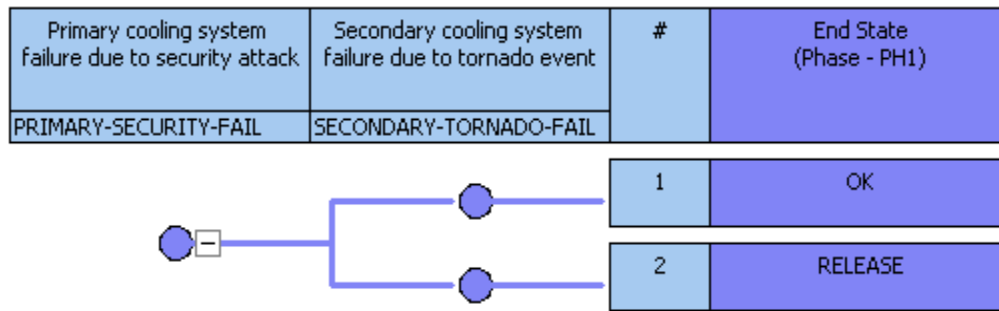
Fig. 31 Cooling system failure due to security sabotage with tornado

The frequency of tornado is considered to be **2.20E-07** per year [13]. The joint failure frequency calculation is carried out by combining the security attack frequency at the primary cooling system (1.63E-04 per year) with the tornado frequency at the secondary cooling system (2.20E-07 per year), which is **3.58E-11** per year. Note: if the scenario were changed as the security attack happening at the secondary cooling system with tornado at the primary cooling system, this gives the same joint failure frequency value (because the security attack event and the tornado have fixed frequency values).

4.1.6. Cooling system failure due to security sabotage in conjunction with an aircraft crash

In this scenario, a security sabotage attack caused failure at the primary cooling system, which is accompanied by failure of the secondary cooling system due to an aircraft crash event. The event tree constructed for this scenario is shown in Fig. 32.
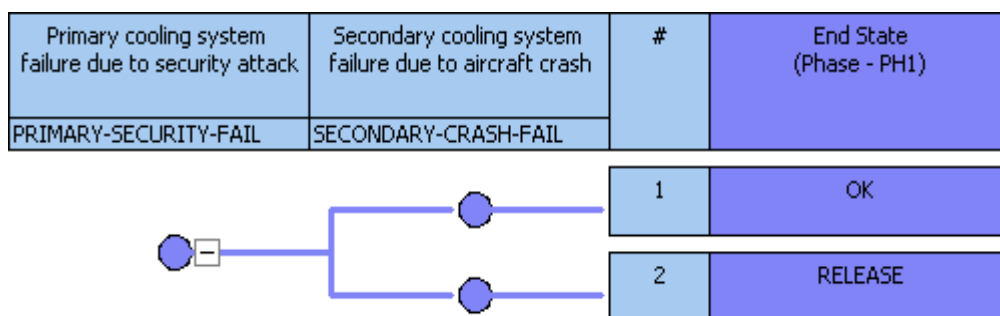
Fig. 32 Cooling system failure due to security attack with aircraft crash

The frequency of aircraft crash in to or near a spent fuel pool is considered to be **7.0E-07** per year [13]. The joint frequency of failure calculation is found by combining the security attack frequency at the primary cooling system (1.63E-04 per year) with the aircraft crash frequency at the secondary cooling system (7.0E-07 per year), which is **1.14E-10** per year. Note: if the scenario were changed as the security attack happening at the secondary cooling system with aircraft crash at the primary cooling system, this gives the same joint failure frequency value (because the security attack event and the aircraft crash have fixed frequency values).

4.2. Combined Safety-Security Cooling System Failure Risk Estimation

As pointed out before in section-1, the consequence value C is common between safety and security as both affect the public domain. Using Eq .7 with a level 4 accident on the INES scale, the associated consequence value C is 8.0E-4. The risk value associated with the scenario of failure estimated by multiplying the consequence value with the failure frequency using Eq .2. Table 5 summarizes the combined failure frequency

and the combined risk estimates of the safety-security failure scenarios analyzed in sub-sections 4.1.1-4.

Table 5 Combined failure frequencies and risk values of the safety-security failure scenarios

S/ No.	Scenario Description	IE Failure Frequency/ y	Total Failure Frequency/ y	Risk / y
1.	Security event at the primary and natural failure of the secondary	1.63E-04	1.47E-13	1.17E-16
2.	Natural failure of the primary and security event at the secondary	1.63E-04	2.14E-6	1.71E-09
3.	Security event at the primary and heavy load drop on secondary or vice versa	1.63E-04	3.42E-09	2.73E-12
4.	Security event at the primary and seismic on secondary or vice versa	1.63E-04	3.28E-10	2.60E-13
5.	Security event at the primary and tornado on secondary or vice versa	1.63E-04	3.58E-11	2.86E-14
6.	Security event at the primary and aircraft crash on secondary or vice versa	1.63E-04	1.14E-10	9.13E-14

4.3. Combined Safety-Security Analysis for Emergency Diesel Generators

The combined methodology, which was developed in this research and applied to the SFP target can be applied to any target in a nuclear facility. For this reason, another

target is considered in this section, which is the Emergency Diesel Generators (EDGs) system. The initiating event for this problem is the Loss of Offsite Power (LOOP). The Emergency Power System (EPS) is assumed to be in the same location of the previous target (SFP) and composed of three Emergency Diesel Generators (EDGs). The security attack frequency is the same for the scenario where any diesel generator or any combination of two diesel generators is attacked by adversaries since they are located at the same location as the SFP.

The scenario assumed in this section is the adversaries attack on the EDGs happens after the LOOP initiating event accompanied with Common Cause Failure (CCF) of one or two EDGs. To calculate the combined failure frequency of such a scenario, the CCF frequencies of the EDGs are required with the previous security attack frequency (1.63E-04 attack per year). The failure frequencies that are considered in this analysis are as follows:

- LOOP frequency is 3.60E-02 f/year.

- Each single failure of any diesel generator is 5.3 f/year

- 2 EDGs out of 3 failure frequency is 0.162 f/year.

- 3 EDGs out of 3 failure frequency is 0.103 f/ year [32].

Since the CCF frequencies are conditional failure based on a blackout case, then the CCFs as follows:

- 1 out of 3 CCF-rate is 1.9E-01 f/year (single failure rate multiplied by the LOOP frequency, it's assumed that the LOOP event and 1 EDG failure to start are independent events).

- 2 out of 3 CCF-rate is 5.83E-03 f/year (considered the combinations of any diesel generators failure, it's assumed that the LOOP event and 2 EDGs failure to start are independent events).

- 3 out of 3 CCF-rate is 3.71E-03 f/year (it's assumed that the LOOP event and 3 EDGs failure to start are independent events).

Two scenarios were considered in this section for EDGs target. The first scenario is that one diesel generator is attacked by the adversaries causing it to fail, accompanied with 2 out of 3 CCF of the EDGs. The event tree constructed for this scenario is shown in Fig. 33.
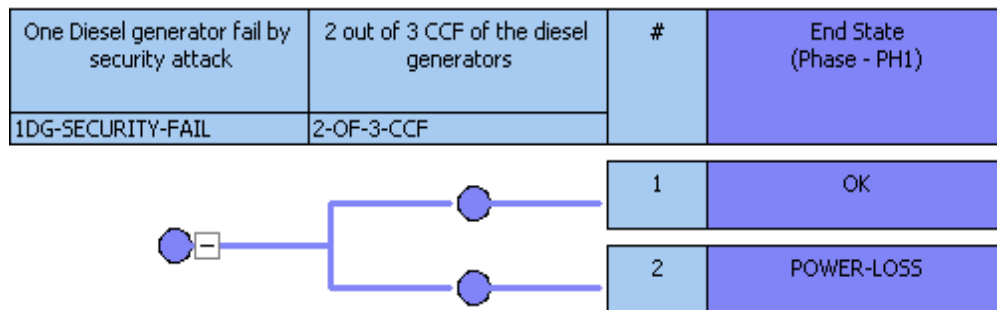
Fig. 33 EDGs failure due to security attack and 2 out of 3 CCF

The combined frequency of failure for this scenario is the multiplication of the security attack frequency (1.63E-04 attack/year) by the 2 out of 3 CCF- rate (5.83E-03 f/year), which gives **1.13E-06** f/year.

The second scenario is described in the event tree in Fig. 34, in which the security attack causing two EDGs to fail accompanied with 1 out of 3 CCF of the EDGs.

Two diesel generators fail by security attack	1 out of 3 CCF of the diesel generators	#	End State (Phase - PH1)
2DG-SECURITY-FAIL	1-OF-3-CCF		
		1	OK
		2	POWER-LOSS
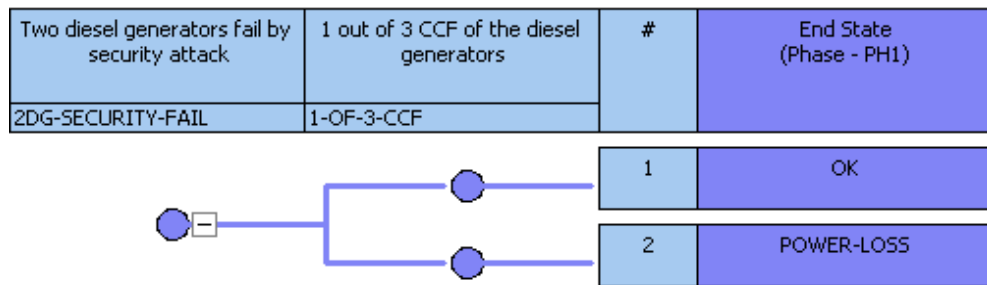
Fig. 34 EDGs failure due to security attack and 1 out of 3 CCF

The combined frequency of failure for this scenario is the multiplication of the security attack frequency (1.63E-04 attack/year) by the 1 out of 3 CCF- rate (1.9E-01 f/year), which gives **3.10 E-05** f/year. The total combined frequency of failure for these two scenarios is the summation of the two scenarios combined frequency of failure (because security attack could happen to 1 **Or** 2 EDGs), which is **3.21** E-05 f/year.

The purpose of this section was to show that this developed methodology can be applied anywhere in the facility to any systems present. Considering the security attack (non-random event) in a random event failure series changes the failure frequency and is known as the combined frequency of failure. In the combined analysis, the security event (non- random event) is considered as a random event in the safety failure series process, which enables the probability multiplication to get the combined failure frequency.

5. RESULTS AND DISCUSSION

This section provides a summary of the results risk values calculated for initiating events of security-type, safety-type and combined security-safety type using a new methodology. The first analysis section was the security pathway analysis, in which the goal was to calculate the security parameters that led to security risk value estimation. This was done by analyzing a specific adversaries' path starting from offsite area toward the target. Table 6 summarizes the calculated security parameters values along with the resulting risk values. As shown in the table, the risk value associated with the security-only scenario, a probable direct attack to the SFP, is estimated to be 1.3E-07 per year. With a uncertainty of 10% assumed in the frequency of attack, P_A the uncertainty in security risk value is very small and can be neglected.

Table 6 Security risk analysis parameters results and uncertainty

Security Parameters	Results	Uncertainty
Frequency of attack (attack / year)	1.0E-03	1.0E-04
Probability of interruption	0.89	5.4E-02
Probability of neutralization	0.94	9.4E-02
Consequence	8.0E-04	8.0E-05
Frequency of security event (successful attack / year)	1.63E-04	1.0E-05
Security Risk (year)	1.3E-07	1.52E-08

For a different path, the risk value changes because at each path the security parameters have different values based on the deployed security systems. The P_I value depends on the probability of detection and the time delay that each protection element provides between the physical protection layers. The P_N value depends on the capabilities, tactics and strength of both the adversaries and the response force during the engagement.

Safety and safety-security analyses were applied to the SFP cooling system to calculate the failure frequency of the system based on different failure scenarios. The cooling system is composed of a primary and a secondary system. The primary cooling system's natural failure is 1.31E-02 per year, while the secondary cooling system's natural failure frequency is 9.0E-10 per year (the failure frequency of the system depends on the individual components' failure frequencies). Table 7 summarizes the risk value for all the cases that were analyzed in this research along with the uncertainty in the risk values, which is calculated by applying Eq.6

Based on the risk values one can note that the safety system showed high reliability conditions because the resulting risk value for a pure natural failure of the safety cooling system was 9.44E-15 per year. The safety failure frequencies are so small because they are dominated by a combination of pumps, each with a failure frequency of 3.0E-05 per year and a consequence value of 8.0E-04. The total risk value is calculated by the summation of risk values associated with all of the possible failure events. The security attack risk values are higher than the natural safety failure by a factor of 1.0**E+08**, causing a significant impact on the system total risk value. The security attack event dominated the combined safety-security analysis risk values. For example, it changed the complete

66

system natural failure from 9.44E-15 per year to 1.71E-09 per year, a factor of 1.0**E+06**, when a security attack caused the secondary cooling system to fail rather than a natural failure. Based on this result, it should be a requirement for future analysts to consider the deployed security systems in the analysis process in order to provide a better estimation of the total risk value.

A heavy load drop, seismic was considered as an external initiating event that can cause the cooling system to fail, along with a natural mechanical failure of the system components. A heavy load drop on the secondary cooling system and natural failure of the primary cooling system resulted in a failure frequency value of 2.20E-10 per year for the cooling system, higher than the failure frequency value of the seismic initiating event. A security event affected and increased the total resulting value of failure frequency when combined with a heavy load drop, seismic, tornado, aircraft events. A tornado and aircraft crash were analyzed to show that different initiating events could be considered in order to find the total risk value.

The uncertainty results show very small error values, which range from 10 to 20% of the calculated values. Therefore, it can be neglected because it has minor effects on the calculated failure frequencies and their associated risk values. The next section provides more illustrations about the uncertainty calculations in this research.

Table 7 Summary of the analyzed scenarios risk values and uncertainty

S/No	Scenario Description	Risk / y	Uncertainty /y
1.	Pure security attack	1.3E-07	1.52E-08
2.	Cooling system all natural safety failure	9.44E-15	1.85E-15
3.	Heavy load drop on the primary and natural failure of the secondary systems	1.51E-17	3.0E-18
4.	Heavy load drop on the secondary system and natural failure of the primary system	2.20E-10	3.81E-11
5.	Seismic event on the primary system and natural failure of the secondary system	1.44E-18	2.87E-19
6.	Seismic event on the secondary system and natural failure of the primary system	2.09E-11	8.13E-12
7.	Security event at the primary and natural failure of the secondary	1.17E-16	2.14E-17
8.	Security event at the secondary and natural failure of the primary	1.71E-09	2.64E-10
9.	Security event at the primary and heavy load drop on secondary or vice versa	2.73E-12	4.20E-13
10.	Security event at the primary and seismic on secondary or vice versa	2.60E-13	4.68E-14
11.	Security event at the primary and tornado on secondary or vice versa	2.86E-14	5.16E-15
12.	Security event at the primary and aircraft crash on secondary or vice versa	9.13E-14	1.64E-14

5.1 Uncertainties of the Frequency of Failure and the Estimated Risk Values

The calculated failure frequency values and the estimated risk values for any specific component are subjected to uncertainties. The uncertainty value of the total frequency of failure and its associated risk value depend on the uncertainty of the individual component's failure frequency. The uncertainty of frequency of failure for each individual component (such as: frequency of failure for valves, pumps, etc.) is assumed to be 10% of its value (ex. the pump failure frequency is 3.0E-05 per year and the uncertainty in it is 3.0E-6. The valve failure frequency is 1.3E-02 per year and its uncertainty is 1.3E-03 per year), since many instrument vendors provides components with failure frequency uncertainty between 10-20% to reflect its reliability.

The uncertainty of the total failure frequency and the associated risk value were calculated using Eq.5 (since most of the frequency calculation operations were multiplications). The following is an example that shows the uncertainty calculation for the total failure frequency and its associated risk value for scenario-1 results that is summarized in Table 4 (see section 3.4) of the safety analysis section in this research:

The total frequency of failure of scenario-1 is 1.18E-11 per year, this value is the result of multiplying the natural frequency of failure of the primary cooling system times the natural frequency of failure of the secondary cooling system (1.31E-2 * 9.0E-10). The uncertainty of failure frequency of the primary is 1.31E-03 per year (10% of the frequency of failure). The uncertainty of failure frequency of the secondary cooling system, depends on the failure frequency uncertainty of each pump (which is 3.0E-6 per year as assumed

69

before), using Eq.5 the uncertainty of the secondary cooling system frequency of failure is 1.27E-10 per year. Applying Eq.5 again to get the uncertainty of scenario -1 frequency of failure (all safety natural failure for the cooling system) gives the uncertainty value of 2.0E-12 per year.

Now, the uncertainty of scenario-1 risk value, coming from the uncertainty in the consequence value is 8.0E-5 (10% of the consequence value), and the uncertainty of the total failure frequency value of scenario-1 in Table 4, that was just calculated. Applying Eq.5 again, the uncertainty of the first scenario risk value in Table 4 is 1.85E-15 per year. The uncertainty results for the analyzed scenarios in this research are summarized in the previous Table 7.

6. CONCLUSION

This research contained three major analysis sections: security, safety, and safety-security risk analysis to study and analyze possible SFP accident scenarios to evaluate the proposed methodology of combined safety-security risk analysis. In previous works, safety and security risk analysis were done separately without interface. However, this thesis study brought out a methodology to perform combined security-safety risk analysis. The results of this applied new methodology clearly showed the importance of determining joint failure frequency of the top event from a combination of security and safety-type initiating events.

The first analysis section was the security pathway analysis, in which the goal was to calculate the security parameters that led to the security risk value estimation. This was done by analyzing a specific adversary's path from the offsite area to the target, addressing the detection and delay elements with their respective values of probability of detection and time delay. Analysis of the security path allowed for calculation of risk parameters such as the probabilities of interruption and neutralization, which led to the calculation of the initiating event frequency of a successful adversary attack on the spent fuel pool facility as 1.63E-04 per year.

A methodology to assess the combined security-safety risk values associated with either a security initiating event or a safety initiating event was established and demonstrated for the case of a spent nuclear fuel pool. This was possible because the consequence value is shared between the safety and security risk equations. PRA Level-

1 was used for the safety analysis as well as the safety-security joint analysis sections in this research in order to calculate the associated system frequency of failure. The safety analysis represents a series of natural safety systems failure events, either a natural mechanical failure or a failure due to external events such as heavy load drop, seismic, and aircraft crash. On the other hand, the safety-security analysis considered a security initiating event followed by safety systems failure. The PRA analysis included fault and event trees formation, which were used for the description of failure scenarios from the basic event to the top event and calculation of the related frequency of failure of the analyzed system elements. The event and fault trees were formed using SAPHIRE software, which assisted the evaluation process of the chosen failure scenarios.

The main outcomes from this research were the calculation of the combined system failure frequency using a proposed new methodology, the estimation of the public risk associated with failure scenarios, and the determination of how much considering a security event in a series of safety events failure affect the total risk value. The safety analysis section analyzed the natural failure scenario for primary and secondary cooling system based on the individual components failure frequency combinations. The natural failure frequency of the primary cooling system was calculated to be 1.31 E-02 per year, while the secondary cooling system natural failure frequency was calculated to be 9.0E-10 per year. The total natural safety failure of the cooling system resulted in a failure frequency of 1.18 E-11 per year. The pure safety analysis showed a reliable system with a very low public risk value of 9.44 E-15 per year. All the uncertainty values were in the

72

range of 10-20% of the actual calculated values of the frequency of failure and its associated risk, which can be neglected since it has no major effects on the final results.

Considering the security attack as an initiating event that triggers system failure was the implementation of this research methodology that led to the combined safety-security risk analysis estimation. Inserting the security initiating event changed the public risk value in some previously analyzed cases by a factor of E+06 as an example the safety natural failure of cooling system changed from 9.44E-15 per year to 1.71E-09 per year when considering the security attack as the failure reason of the secondary cooling system.

In Conclusion, the analysis showed that the security attack changed the risk value when considered in the failure process of the total system, creating a need to consider the security analysis in real cases with safety-security interfaces. More evaluation should be done to the security system measures in order to reduce the total associated risk value and provide item risk reduction. Future efforts should attempt further enhancement and development in the analysis of the deployed safety and security systems.

REFERENCES

1- BOHN M. P. and LAMBRIGHT J. A., "Procedure for the External Event Core Damage Frequency Analysis for NUREG-1150", *NUREG/CR-4840; SAND88-3102*, November (1990).

2- KIRCHSTEIGER C., "On the Use of Probabilistic and Deterministic Methods in Risk Analysis,", *Journal of Loss Prevention*, *12*(1), 399-419, (1999).

3- GARCIA M. L., *The Design and Evaluation of Physical Protection Systems*, Butterworth Heinemann, Boston, Second Edition (2008).

4- HELSBY G. H. and WHITE R. F., "Criteria for Use in the Assessment and Control of Major Hazards,", *Inst. Chem. E. Symposium Series No. 93*, P. 274 Manchester, (1985).

5- VAN DER MEULEN M., "*Definitions for Hardware and Software Safety Engineers,"*, Springer, London (2012).

6- LINE M. B., NORDLAND O., ROSTAD L., and TONDEL I. A., "Safety vs. Security in the Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management,", *PSAM 2006*, New Orleans, Louisiana, USA, (2006).

7- LUDOVIC P. and CLAUDE C., "The SEMA Referential Framework: Avoiding Ambiguities in the Terms Security and Safety,", *International Journal of Critical Infrastructure Protection, 3*, 55-66, (2010).

8- CIPOLLARO A. and LOMONACO G., "Contributing to the Nuclear 3S's via a Methodology Aiming at Enhancing the Synergies between Nuclear Security and Safety,", *Progress in Nuclear Energy, 86*, 31-39, (2016).

9- CIPOLLARO A., Nuclear Safety, Security and Safeguards: Facets of One Same Challenge for the Future of Nuclear Power,", Ph.D. Thesis, Supervisors: MAZZINI M, PETRANGELI G, LOMONACO G, University of Pisa, (2015).

10- HAWILA M., CHIRAYATH S., and CHARLTON W., "Nuclear Security Risk Evaluation Using Adversary Pathway Analysis Methodology for an Insider-Outsider Collusion Scenario,", *INMM 56th annual proceedings*, Indian wells, California USA July (2015).

11- HAWILA M. and CHIRAYATH S. "*Nuclear Security risk Analysis: An Insider-Outsider Collusion Scenario,*", International Journal of Nuclear Security, Vol.1 No.2, (2016)

12- KIM K. N., SUH Y. A., YIM M. S., and SCHNEIDER E., "Physical Protection System Design Analysis against Insider Threat based on Game Theoretic Modeling,", *Proceedings of the KNS*, spring meeting, (2015).

13- COLLINS T. E. and HUBBARD G., "Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plants,", *NUREG-1738*, (2000).

14- IDAHO NATIONAL LABORATORIES, "System Analysis Programs for Hand-on Integrated Reliability Evaluations (SAPHIRE),", version 8, August (2008).

15- CHIRAYATH S., "Nuclear Fuel Cycles and Materials Safeguards (651 class),", Nuclear Engineering Department, Texas A&M University, Spring Semester (2016).

16- ALVARES R, "Spent Nuclear Fuel in the U.S: Reducing the Deadly Risks of Storage,", *Institute of Policy Studies*, Vol.22, No .5, May (2011).

17- US-NRC," Spent Fuel Generation and Storage After Use", July (2016). http://www.nrc.gov/images/waste/spent-fuel-storage/generation-storage.gif

18- COX, JR, ANTHONY L, "Some limitations of 'Risk = Threat x Vulnerability x Consequence' for Risk Analysis of Terrorist Attacks", *Risk Anal. 28(6):1749-61.* December (2008).

19- SNELL M. K., "Report on Project Action Sheet PP05 Task 3 between the U.S. Department of Energy and the Republic of Korea Ministry of Education, Science, and Technology (MEST),", SANDIA Report SAND2013-0039, January (2013).

20- NUCLEAR SECURITY SCIENCE & POLICY INSTITUTE (NSSPI), "Information Belongs to NSSPI division in Nuclear Engineering Department", Nuclear Engineering Department, College Station, Texas.

21- IAEA, "The Physical Protection of Nuclear Material and Nuclear Facilities,", INFCIRC/225/Rev.4, June (1999).

22- CHIRAYATH S, Private Communication at Texas A&M University, College Station (2016).

23- INTERNATIONAL ATOMIC ENERGY COMMISSION, International Nuclear and radiological event scale (INES), user's manual, Vienna, (2013).

24- USNRC, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995", *NUREG/CR-5750, INEEL/EXT-98-00401*, February (1999).

25- IAEA, "Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants,", *IAEA-TECDOC-1511*, July (2006).

26- SHAUKAT S. K, Jackson J. E, "Regulatory Analysis for Generic Issue 23: Reactor Coolant Pump Seal Failure,", *NUREG-1401*, April (2012).

27- HEALTH AND SAFETY EXECUTIVE (HSE), "Failure Rates and Event Data for Use within Risk Assessments,", PCAG Chp-6k, version 12, June (2012).

28- USNRC, "Industry- Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,", *NUREG/CR-6928, INL/EXT-06-11119*, February (2007).

29- KUZMINA I, IAEA "Basic Risk Concepts and Techniques: Safety Assessment Workshop for the Jordan Nuclear Regulatory Commission," Amman / Jordan, November (2012).

30- USNRC, "Fault Tree Handbook," NUREG-0492, January (1981).

31- AMERICAN BUREAU OF SHIPPING (ABS), "Risk Assessment Applications for the Marine and Offshore Oil and Gas Industries,", June (2000).

32- CAVALUZZI J, "Time-Based Risk-Informed Safety Margins: Concepts and Application to Heterogeneous Systems,", M.S. Thesis, Nuclear Engineering, Texas A&M University, College Station, Texas, (2015.